Management Software

AT-S63

Command Line Interface User's Guide

AT-9400 Series Layer 2+ Gigabit Ethernet Switches

Version 1.3.0

613-50571-00 Rev. D

Allied Telesyn

Copyright © 2005 Allied Telesyn, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesyn, Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesyn, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesyn, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface 15
How This Guide is Organized 16
Document Conventions 17
Where to Find Web-based Guides 18
Contacting Allied Telesyn 19
Online Support 19
Email and Telephone Support 19
Returning Products 19
Sales or Corporate Information 19
Management Software Updates 19
New Features History 20
AT-S63 Version 1.3.0 20
AT-S63 Version 1.2.0 21

Section I: Basic Operations 23

Chapter 1: Starting a Command Line Management Session 25
Starting a Command Line Management Session 26
Command Line Interface Features 27
Command Formatting 28
Ports 23R and 24R on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series Switches 29

Chapter 2: Basic Command Line Commands 31
CLEAR SCREEN 32
EXIT 33
HELP 34
LOGOFF, LOGOUT and QUIT 35
MENU 36
SAVE CONFIGURATION 37
SET PROMPT 38
SET SWITCH CONSOLEMODE 39
SHOW USER 40

Chapter 3: Basic Switch Commands 41
DISABLE DHCPBOOTP 43
DISABLE IP REMOTEASSIGN 44
DISABLE TELNET 45
ENABLE BOOTP 46
ENABLE DHCP 47
ENABLE IP REMOTEASSIGN 48
ENABLE TELNET 49
PING 50
PURGE IP 51
RESET SWITCH 52
RESET SYSTEM 53
RESTART REBOOT 54

RESTART SWITCH 55
SET ASYN 57
SET IP INTERFACE 58
SET IP ROUTE 60
SET PASSWORD MANAGER 61
SET PASSWORD OPERATOR 62
SET SWITCH CONSOLETIMER 63
SET SYSTEM 64
SET TELNET INSERTNULL 65
SET USER PASSWORD 66
SHOW ASYN 67
SHOW CONFIG DYNAMIC 68
SHOW CONFIG INFO 71
SHOW DHCPBOOTP 72
SHOW IP INTERFACE 74
SHOW IP ROUTE 75
SHOW SWITCH 76
SHOW SYSTEM 79

Chapter 4: Enhanced Stacking Commands 81
ACCESS SWITCH 82
SET SWITCH STACKMODE 84
SHOW REMOTELIST 86

Chapter 5: Simple Network Time Protocol (SNTP) Commands 89
ADD SNTPSERVER PEER|IPADDRESS 90
DELETE SNTPSERVER PEER|IPADDRESS 91
DISABLE SNTP 92
ENABLE SNTP 93
PURGE SNTP 94
SET DATE 95
SET SNTP 96
SET TIME 97
SHOW SNTP 98
SHOW TIME 100

Chapter 6: SNMPv2 and SNMPv2c Commands 101
ADD SNMP COMMUNITY 102
CREATE SNMP COMMUNITY 104
DELETE SNMP COMMUNITY 107
DESTROY SNMP COMMUNITY 109
DISABLE SNMP 110
DISABLE SNMP AUTHENTICATETRAP 111
DISABLE SNMP COMMUNITY 112
ENABLE SNMP 113
ENABLE SNMP AUTHENTICATETRAP 114
ENABLE SNMP COMMUNITY 115
SET SNMP COMMUNITY 116
SHOW SNMP 118

Chapter 7: Port Parameter Commands 121
ACTIVATE SWITCH PORT 122
DISABLE INTERFACE LINKTRAP 123
DISABLE SWITCH PORT 124
DISABLE SWITCH PORT FLOW 125
ENABLE INTERFACE LINKTRAP 126
ENABLE SWITCH PORT 127

ENABLE SWITCH PORT FLOW 128
PURGE SWITCH PORT 129
RESET SWITCH PORT 130
SET SWITCH PORT 131
SET SWITCH PORT FILTERING 135
SET SWITCH PORT RATELIMITING 138
SHOW INTERFACE 141
SHOW SWITCH PORT 143

Chapter 8: Port Statistics Commands 149
RESET SWITCH PORT COUNTER 150
SHOW SWITCH COUNTER 151
SHOW SWITCH PORT COUNTER 154

Chapter 9: MAC Address Table Commands 155
ADD SWITCH FDB|FILTER 156
DELETE SWITCH FDB|FILTER 158
RESET SWITCH FDB 160
SET SWITCH AGINGTIMER|AGEINGTIMER 161
SHOW SWITCH AGINGTIMER|AGEINGTIMER 162
SHOW SWITCH FDB 163

Chapter 10: Static Port Trunking Commands 167
ADD SWITCH TRUNK 168
CREATE SWITCH TRUNK 170
DELETE SWITCH TRUNK 172
DESTROY SWITCH TRUNK 173
SET SWITCH TRUNK 174
SHOW SWITCH TRUNK 175

Chapter 11: LACP Port Trunking Commands 177
ADD LACP PORT 178
CREATE LACP AGGREGATOR 179
DELETE LACP PORT 181
DESTROY LACP AGGREGATOR 182
DISABLE LACP 183
ENABLE LACP 184
SET LACP AGGREGATOR 185
SET LACP SYSPRIORITY 187
SET LACP STATE 188
SHOW LACP 189

Chapter 12: Port Mirroring Commands 193
SET SWITCH MIRROR 194
SET SWITCH PORT MIRROR 195
SHOW SWITCH MIRROR 196

Chapter 13: Networking Stack 197
DELETE IP ARP 198
DELETE TCP 199
RESET IP ARP 200
SET IP ARP TIMEOUT 201
SHOW IP ARP 202
SHOW IP ROUTE 203
SHOW TCP 204

Section II: Advanced Operations 207

Chapter 14: File System Commands 209
COPY 210
CREATE CONFIG 212
DELETE FILE 213
FORMAT DEVICE 215
RENAME 216
SET CFLASH DIR 218
SET CONFIG 219
SHOW CFLASH 221
SHOW CONFIG 222
SHOW FILE 223
SHOW FLASH 224

Chapter 15: File Download and Upload Commands 225
LOAD METHOD=LOCAL 226
LOAD METHOD=TFTP 228
LOAD METHOD=XMODEM 232
UPLOAD METHOD=LOCAL 236
UPLOAD METHOD=REMOTESWITCH 238
UPLOAD METHOD=TFTP 243
UPLOAD METHOD=XMODEM 246

Chapter 16: Event Log and Syslog Server Commands 249
ADD LOG OUTPUT 250
CREATE LOG OUTPUT 252
DESTROY LOG OUTPUT 256
DISABLE LOG 257
DISABLE LOG OUTPUT 258
ENABLE LOG 259
ENABLE LOG OUTPUT 260
PURGE LOG 261
SAVE LOG 262
SET LOG FULLACTION 264
SET LOG OUTPUT 265
SHOW LOG 268
SHOW LOG OUTPUT 273
SHOW LOG STATUS 275

Chapter 17: Classifier Commands 277
CREATE CLASSIFIER 278
DESTROY CLASSIFIER 282
PURGE CLASSIFIER 283
SET CLASSIFIER 284
SHOW CLASSIFIER 287

Chapter 18: Access Control List Commands 289
CREATE ACL 290
DESTROY ACL 292
PURGE ACL 293
SET ACL 294
SHOW ACL 296

Chapter 19: Class of Service (CoS) Commands 299
MAP QOS COSP 300
PURGE QOS 302
SET QOS COSP 303
SET QOS SCHEDULING 304
SET SWITCH PORT PRIORITY OVERRIDEPRIORITY 305
SHOW QOS CONFIG 307

Chapter 20: Quality of Service (QoS) Commands 309
ADD QOS FLOWGROUP 310
ADD QOS POLICY 311
ADD QOS TRAFFICCLASS 312
CREATE QOS FLOWGROUP 313
CREATE QOS POLICY 316
CREATE QOS TRAFFICCLASS 323
DELETE QOS FLOWGROUP 328
DELETE QOS POLICY 329
DELETE QOS TRAFFICCLASS 330
DESTROY QOS FLOWGROUP 331
DESTROY QOS POLICY 332
DESTROY QOS TRAFFICCLASS 333
PURGE QOS 334
SET QOS FLOWGROUP 335
SET QOS POLICY 338
SET QOS PORT 341
SET QOS TRAFFICCLASS 342
SHOW QOS FLOWGROUP 347
SHOW QOS POLICY 349
SHOW QOS TRAFFICCLASS 351

Chapter 21: Denial of Service Defense Commands 353
SET DOS 354
SET DOS IPOPTION 355
SET DOS LAND 357
SET DOS PINGOFDEATH 358
SET DOS SMURF 360
SET DOS SYNFLOOD 361
SET DOS TEARDROP 362
SHOW DOS 364

Section III: IGMP Snooping, MLD Snooping, and RRP Snooping 367

Chapter 22: IGMP Snooping Commands 369
DISABLE IGMPSNOOPING 370
ENABLE IGMPSNOOPING 371
SET IP IGMP 372
SHOW IGMPSNOOPING 375
SHOW IP IGMP 376

Chapter 23: MLD Snooping Commands 379
DISABLE MLDSNOOPING 380
ENABLE MLDSNOOPING 381
SET IPV6 MLDSNOOPING 382
SHOW MLDSNOOPING 384
SHOW IPV6 MLDSNOOPING 386

Chapter 24: RRP Snooping Commands 389
DISABLE RRPSNOOPING 390
ENABLE RRPSNOOPING 391
SHOW RRPSNOOPING 392

Section IV: SNMPv3 393

Chapter 25: SNMPv3 Commands 395
ADD SNMPV3 USER 397
CLEAR SNMPV3 ACCESS 399
CLEAR SNMPV3 COMMUNITY 401
CLEAR SNMPV3 NOTIFY 402
CLEAR SNMPV3 TARGETADDR 403
CLEAR SNMPV3 VIEW 404
CREATE SNMPV3 ACCESS 405
CREATE SNMPV3 COMMUNITY 408
CREATE SNMPV3 GROUP 410
CREATE SNMPV3 NOTIFY 412
CREATE SNMPV3 TARGETADDR 414
CREATE SNMPV3 TARGETPARAMS 416
CREATE SNMPV3 VIEW 418
DELETE SNMPV3 USER 420
DESTROY SNMPv3 ACCESS 421
DESTROY SNMPv3 COMMUNITY 423
DESTROY SNMPv3 GROUP 424
DESTROY SNMPv3 NOTIFY 425
DESTROY SNMPv3 TARGETADDR 426
DESTROY SNMPv3 TARGETPARMS 427
DESTROY SNMPV3 VIEW 428
PURGE SNMPV3 ACCESS 429
PURGE SNMPV3 COMMUNITY 430
PURGE SNMPV3 NOTIFY 431
PURGE SNMPV3 TARGETADDR 432
PURGE SNMPV3 VIEW 433
SET SNMPV3 ACCESS 434
SET SNMPV3 COMMUNITY 436
SET SNMPV3 GROUP 438
SET SNMPV3 NOTIFY 440
SET SNMPV3 TARGETADDR 442
SET SNMPV3 TARGETPARAMS 444
SET SNMPV3 USER 446
SET SNMPV3 VIEW 448
SHOW SNMPV3 ACCESS 450
SHOW SNMPV3 COMMUNITY 451
SHOW SNMPv3 GROUP 452
SHOW SNMPV3 NOTIFY 453
SHOW SNMPV3 TARGETADDR 454
SHOW SNMPV3 TARGETPARAMS 455
SHOW SNMPV3 USER 456
SHOW SNMPV3 VIEW 457

Section V: Spanning Tree Protocols 459

Chapter 26: Spanning Tree Protocol Commands 461
ACTIVATE STP 462
DISABLE STP 463
ENABLE STP 464
PURGE STP 465
SET STP 466
SET STP PORT 469
SET SWITCH MULTICASTMODE 471
SHOW STP 473

Chapter 27: Rapid Spanning Tree Protocols Commands 475
ACTIVATE RSTP 476
DISABLE RSTP 477
ENABLE RSTP 478
PURGE RSTP 479
SET RSTP 480
SET RSTP PORT 483
SHOW RSTP 486

Chapter 28: Multiple Spanning Tree Protocol Commands 489
ACTIVATE MSTP 490
ADD MSTP 491
CREATE MSTP 492
DELETE MSTP 493
DESTROY MSTP MSTIID 494
DISABLE MSTP 495
ENABLE MSTP 496
PURGE MSTP 497
SET MSTP 498
SET MSTP CIST 501
SET MSTP MSTI 502
SET MSTP MSTIVLANASSOC 504
SET MSTP PORT 505
SHOW MSTP 509

Section VI: Virtual LANs 513

Chapter 29: Port-based, Tagged, and Multiple Mode VLAN Commands 515
ADD VLAN 516
CREATE VLAN 518
DELETE VLAN 521
DESTROY VLAN 523
SET SWITCH INFILTERING 524
SET SWITCH MANAGEMENTVLAN 525
SET SWITCH VLANMODE 526
SET VLAN 528
SHOW VLAN 529

Chapter 30: GARP VLAN Registration Protocol Commands 533
DISABLE GARP 534
ENABLE GARP 535
PURGE GARP 536
SET GARP PORT 537
SET GARP TIMER 538

SHOW GARP 540
SHOW GARP COUNTER 541
SHOW GARP DATABASE 543
SHOW GARP GIP 544
SHOW GARP MACHINE 545

Chapter 31: Protected Ports VLAN Commands 547
ADD VLAN GROUP 548
CREATE VLAN PORTPROTECTED 550
DELETE VLAN 551
DESTROY VLAN 553
SET VLAN 554
SHOW VLAN 555

Chapter 32: MAC Address-based VLAN Commands 557
ADD VLAN MACADDRESS 558
ADD VLAN PORT MACADDRESS 559
CREATE VLAN TYPE=MACADDRESS 560
DELETE VLAN MACADDRESS 562
DELETE VLAN PORT MACADDRESS 563
DESTROY VLAN 564
SHOW VLAN 565

Section VII: Port Security 567

Chapter 33: MAC Address-based Port Security Commands 569
SET SWITCH PORT INTRUSIONACTION 570
SET SWITCH PORT SECURITYMODE 571
SHOW SWITCH PORT INTRUSION 574
SHOW SWITCH PORT SECURITYMODE 575

Chapter 34: 802.1x Port-based Network Access Control Commands 577
DISABLE PORTACCESS|PORTAUTH 578
DISABLE RADIUSACCOUNTING 579
ENABLE PORTACCESS|PORTAUTH 580
ENABLE RADIUSACCOUNTING 581
SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR 582
SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT 590
SET RADIUSACCOUNTING 592
SHOW PORTACCESS|PORTAUTH 594
SHOW PORTACCESS|PORTAUTH PORT 596
SHOW RADIUSACCOUNTING 599

Section VIII: Management Security 601

Chapter 35: Web Server Commands 603
DISABLE HTTP SERVER 604
ENABLE HTTP SERVER 605
PURGE HTTP SERVER 606
SET HTTP SERVER 607
SHOW HTTP SERVER 612

Chapter 36: Encryption Key Commands 613
CREATE ENCO KEY 614
DESTROY ENCO KEY 618
SET ENCO KEY 619
SHOW ENCO 620

Chapter 37: Public Key Infrastructure (PKI) Certificate Commands 621
ADD PKI CERTIFICATE 622
CREATE PKI CERTIFICATE 624
CREATE PKI ENROLLMENTREQUEST 627
DELETE PKI CERTIFICATE 629
PURGE PKI 630
SET PKI CERTIFICATE 631
SET PKI CERTSTORELIMIT 633
SET SYSTEM DISTINGUISHEDNAME 634
SHOW PKI 635
SHOW PKI CERTIFICATE 636

Chapter 38: Secure Sockets Layer (SSL) Commands 637
SET SSL 638
SHOW SSL 639

Chapter 39: Secure Shell (SSH) Commands 641
DISABLE SSH SERVER 642
ENABLE SSH SERVER 643
SET SSH SERVER 646
SHOW SSH 648

Chapter 40: TACACS+ and RADIUS Commands 649
ADD RADIUSSERVER 650
ADD TACACSSERVER 652
DELETE RADIUSSERVER 653
DELETE TACACSSERVER 654
DISABLE AUTHENTICATION 655
ENABLE AUTHENTICATION 656
PURGE AUTHENTICATION 657
SET AUTHENTICATION 658
SHOW AUTHENTICATION 660

Chapter 41: Management ACL Commands 661
ADD MGMTACL 662
CREATE MGMTACL 663
DESTROY MGMTACL 665
DISABLE MGMTACL 666
ENABLE MGMTACL 667
PURGE MGMTACL 668
SET MGMTACL 669
SHOW MGMTACL 670

Index 671

Tables

Table 1. New Features in AT-S63 Version 1.3.0 20
Table 2. New Features in AT-S63 Version 1.2.0 21
Table 3. Module Variable 68
Table 4. File Extensions and File Types 210
Table 5. File Name Extensions - Downloading Files 229
Table 6. File Name Extensions - Uploaded Files 244
Table 7. Default Syslog Facilities 254
Table 8. Numerical Code and Facility Level Mappings 254
Table 9. AT-S63 Modules 269
Table 10. Event Log Severity Levels 271
Table 11. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues 300
Table 12. Bridge Priority Value Increments 466
Table 13. STP Auto-Detect Port Costs 469
Table 14. Auto-Detect Port Trunk Costs 469
Table 15. Port Priority Value Increments 470
Table 16. Bridge Priority Value Increments 480
Table 17. RSTP Auto-Detect Port Costs 483
Table 18. RSTP Auto-Detect Port Trunk Costs 483
Table 19. Port Priority Value Increments 484
Table 20. CIST Priority Value Increments 501
Table 21. MSTI Priority Value Increments 502
Table 22. Auto External Path Costs 505
Table 23. Auto External Path Trunk Costs 505
Table 24. Port Priority Value Increments 507

Preface

This guide contains instructions on how to configure and maintain an AT-9400 Series Layer 2+ Gigabit Ethernet switch using the command line interface in the AT-S63 management software.

For instructions on how to manage the switch from the menus or web browser interface, refer to the *AT-S63 Management Software Menus Interface User's Guide* or the *AT-S63 Management Software Web Browser Interface User's Guide*. The guides are available from the Allied Telesyn web site.

For background information and guidelines on the features of the AT-9400 Series switches and the AT-S63 management software, refer to the appropriate chapter in the *AT-S63 Management Software Menus Interface User's Guide*. This guide also contains an overview of the different methods to managing a switch.

This Preface contains the following sections:

- ❒ "How This Guide is Organized" on page 16
- ❒ "Document Conventions" on page 17
- ❒ "Where to Find Web-based Guides" on page 18
- ❒ "Contacting Allied Telesyn" on page 19
- ❒ "New Features History" on page 20

Caution

The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a "retail encryption item" in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesyn sales representative for current information on this product's export status.

How This Guide is Organized

This guide is organized into the following sections

- Section I: Basic Operations

  The chapters in this section contain the commands for performing a variety of basic operations, such as configuring a switch's IP configuration, setting port parameters, and using enhanced stacking.

- Section II: Advanced Operations

  The chapters in this section contain the commands for performing different advanced operations, such as managing the file system, uploading and downloading files, using the event log, and working with classifiers and Quality of Service.

- Section III: IGMP Snooping, MLD Snooping, and RRP Snooping

  The chapters in this section contain the commands for configuring IGMP snooping, MLD snooping, and RRP snooping.

- Section IV: SNMPv3

  The chapter in this section contains the commands for configuring SNMPv3.

- Section V: Spanning Tree Protocols

  The chapters in this section contain the commands for configuring the Spanning Tree, Rapid Spanning Tree, and Multiple Spanning Tree Protocols.

- Section VI: Virtual LANs

  The chapters in this section contain the commands for configuring port-based and tagged VLANs, GVRP, protected ports VLANs, MAC address-based VLANs, and multiple VLAN modes.

- Section VII: Port Security

  The chapters in this section contain the commands for configuring MAC address-based security and 802.1x port-based network access control.

- Section VIII: Management Security

  The chapters in this section contain the commands for managing the web server, encryption keys, Public Key Infrastructure certificates, Secure Shell, TACACS+ and RADIUS, and the management access control list.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in portable document format (PDF) on our web site at **www.alliedtelesyn.com**. You can view the documents online or download them onto a local workstation or server.

Contacting Allied Telesyn

This section provides Allied Telesyn contact information for technical support as well as sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base: **http://kb.alliedtelesyn.com**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesyn without an RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact Allied Telesyn Technical Support through our web site: **www.alliedtelesyn.com**.

Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information through our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

New releases of management software for our managed products are available from either of the following Internet sites:

- Allied Telesyn web site: **www.alliedtelesyn.com**
- Allied Telesyn FTP server: **ftp://ftp.alliedtelesyn.com**

If you prefer to download new software from the Allied Telesyn FTP server from your workstation's command prompt, you will need FTP client software and you must log in to the server. Enter "anonymous" for the user name and your email address for the password.

New Features History

AT-S63 Version 1.3.0

Table 1 lists the new features in version 1.3.0 of the AT-S63 management software.

Table 1. New Features in AT-S63 Version 1.3.0

Change	Chapter and Command
Basic Switch Commands	
Modified the SHOW CONFIG DYN command to display the parameter settings of individual switch modules.	Chapter 3, “Basic Switch Commands” on page 41 Modified command: “SHOW CONFIG DYNAMIC” on page 68
802.1x port-based network access control	
Added the following new features: ❒ GUESTVLAN parameter for supporting Guest VLANs. ❒ VLANASSIGNMENT and SECUREVLAN parameters for supporting dynamic VLAN assignments from a RADIUS authentication server for supplicant accounts. ❒ MACBASED parameter for supporting MAC address-based authentication as an alternative to 802.1x username and password authentication.	Chapter 34, “802.1x Port-based Network Access Control Commands” on page 577 Modified command: “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 582
Management Access Control List	
Simplified the commands for managing the access control entries in the Management ACL.	Chapter 41, “Management ACL Commands” on page 661

AT-S63 Version 1.2.0

Table 2 lists the new features in version 1.2.0 of the AT-S63 management software.

Table 2. New Features in AT-S63 Version 1.2.0

Change	Chapter and Command
MAC Address Table	
Added new parameters to the CLI commands for deleting and displaying specific types of MAC addresses in the MAC address table. The new parameters are: ❒ STATIC, STATICUNICAST, and, STATICMULTICAST for deleting and displaying static unicast and multicast MAC addresses. ❒ DYNAMIC, DYNAMICUNICAST, and, DYNAMICMULTICAST for deleting and displaying dynamic unicast and multicast MAC addresses.	Chapter 9, "MAC Address Table Commands" on page 155 Modified commands: "DELETE SWITCH FDB|FILTER" on page 158 "SHOW SWITCH FDB" on page 163
Quality of Service - Flow Groups and Traffic Classes	
Added the following parameters to the commands for creating and modifying flow groups and traffic classes: ❒ TOS parameter for replacing the Type of Service (ToS) field of IPv4 packets. ❒ MOVETOSTOPRIORITY parameter for replacing the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets. ❒ MOVEPRIORITYTOTOS parameter for replacing the value in the ToS priority field with the 802.1p priority field in IPv4 packets.	Chapter 20, "Quality of Service (QoS) Commands" on page 309 Modified commands: "CREATE QOS FLOWGROUP" on page 313 "SET QOS FLOWGROUP" on page 335 "CREATE QOS TRAFFICCLASS" on page 323 "SET QOS TRAFFICCLASS" on page 342

Table 2. New Features in AT-S63 Version 1.2.0 (Continued)

Change	Chapter and Command
❒ **Quality of Service - Policies**	
Added the following parameters to the commands for creating and modifying QoS policies: ❒ TOS, MOVETOSTOPRIORITY and MOVEPRIORITYTOTOS, as defined above. ❒ SENDTOMIRROR parameter for copying traffic to a destination mirror port. (This parameter applies only to QoS policies.)	Chapter 20, “Quality of Service (QoS) Commands” on page 309 Modified commands: “CREATE QOS POLICY” on page 316 “SET QOS POLICY” on page 338
MLD Snooping	
New feature.	Chapter 23, “MLD Snooping Commands” on page 379
MAC address-based VLANs	
New feature.	Chapter 32, “MAC Address-based VLAN Commands” on page 557
802.1x port-based network access control	
Added the following parameter to the command for configuring an authenticator port: ❒ MODE parameter for supporting multiple supplicant accounts on an authenticator port.	Chapter 34, “802.1x Port-based Network Access Control Commands” on page 577 Modified command: “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 582

Section I

Basic Operations

The chapters in this section provide information and procedures for basic switch setup using the AT-S63 management software. The chapters include:

- Chapter 1, “Starting a Command Line Management Session” on page 25
- Chapter 2, “Basic Command Line Commands” on page 31
- Chapter 3, “Basic Switch Commands” on page 41
- Chapter 4, “Enhanced Stacking Commands” on page 81
- Chapter 5, “Simple Network Time Protocol (SNTP) Commands” on page 89
- Chapter 6, “SNMPv2 and SNMPv2c Commands” on page 101
- Chapter 7, “Port Parameter Commands” on page 121
- Chapter 8, “Port Statistics Commands” on page 149
- Chapter 9, “MAC Address Table Commands” on page 155
- Chapter 10, “Static Port Trunking Commands” on page 167
- Chapter 11, “LACP Port Trunking Commands” on page 177
- Chapter 12, “Port Mirroring Commands” on page 193
- Chapter 13, “Networking Stack” on page 197

Chapter 1

Starting a Command Line Management Session

This chapter contains the following topics:

- “Starting a Command Line Management Session” on page 26
- “Command Line Interface Features” on page 27
- “Command Formatting” on page 28
- “Ports 23R and 24R on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series Switches” on page 29

Starting a Command Line Management Session

The command line interface is supported from a local, Telnet, or SSH management session of an AT-9400 Series switch. For instructions on how to start a local or remote management session, refer to the *AT-S63 Management Software Menus Interface User's Guide.*

The default management interface when you start a session is the command line interface (CLI). The prompt differs depending on whether you logged in as manager or operator. If you logged in as manager, you will see "#." If you logged in as operator, you will see "$."

Note
Web browser interface does not support the command line interface.

Command Line Interface Features

The following features are supported in the command line interface:

- Command history - Use the up and down arrow keys.
- Context-specific help - Press the question mark key at any time to see a list of legal next parameters.
- Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix, for example, "sh" for "show".
- Tab key - Pressing the Tab key fills in the rest of the keyword. For example, typing "di" and pressing the Tab key enters "disable."

Command Formatting

The following formatting conventions are used in this manual:

- `screen text font` - This font illustrates the format of a command and command examples.
- *`screen text font`* - Italicized screen text indicates a variable for you to enter.
- [ ] - Brackets indicate optional parameters.
- | - Vertical line separates parameter options for you to choose from.

Ports 23R and 24R on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series Switches

This section applies to the twisted pair ports 23R and 24R and the SFP and GBIC slots on the AT-9424T/GB, AT-9424T/SP, and AT-9424Ti/SP Series switches. Note the following when configuring these ports:

- Twisted pair ports 23R and 24R change to the redundant status mode when an SFP or GBIC module is installed and establishes a link with its end node. An SFP or GBIC port is only active while it has a valid link. At all other times the corresponding twisted pair port 23R or 24R is the active port.
- A twisted pair port and its corresponding SFP or GBIC module share the same configuration settings, including port settings, VLAN assignments, access control lists, and spanning tree. When an SFP or GBIC module becomes active, it operates with the same settings as its corresponding twisted pair port.
- An exception is port speed: If you disable Auto-Negotiation on the twisted pair port and set the speed and duplex mode manually, the speed reverts to Auto-Negotiation when you install an SFP or GBIC module and the module establishes a link with an end node.
- To specify twisted pair port 23R or 24R in a command line command, enter "23" or "24". For example, to change the description of port 23R to "Sales server," you would enter:

  ```
  set switch port=23 description="Sales server"
  ```

Chapter 2

Basic Command Line Commands

This chapter contains the following commands:

- “CLEAR SCREEN” on page 32
- “EXIT” on page 33
- “HELP” on page 34
- “LOGOFF, LOGOUT and QUIT” on page 35
- “MENU” on page 36
- “SAVE CONFIGURATION” on page 37
- “SET PROMPT” on page 38
- “SET SWITCH CONSOLEMODE” on page 39
- “SHOW USER” on page 40

Note
Remember to save your changes with the SAVE CONFIGURATION command.

CLEAR SCREEN

Syntax

```
clear screen
```

Parameters

None.

Description

This command clears the screen.

Example

The following command clears the screen:

```
clear screen
```

EXIT

Syntax

```
exit
```

Parameters

None.

Description

This command ends a management session. If you are managing a slave switch, the command returns you to the master switch from where you started the management session.

Example

The following command ends the current management session:

```
exit
```

Equivalent Commands

```
logoff
```

logout

quit

For information, see "LOGOFF, LOGOUT and QUIT" on page 35.

HELP

Syntax

```
help
```

Parameters

None.

Description

This command displays a list of the CLI keywords with a brief description for each keyword.

Example

The following command displays the CLI keywords:

```
help
```

LOGOFF, LOGOUT and QUIT

Syntax

```
logoff
```

```
logout
```

```
quit
```

Parameters

None.

Description

These three commands all perform the same function: they end a management session. If you are managing a slave switch, the commands return you to the master switch from which you started the management session.

Example

The following command ends a management session:

```
logoff
```

MENU

Syntax

```
menu
```

Parameters

None.

Description

This command displays the AT-S63 Main Menu. For instructions on how to use the menus, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

Example

The following command displays the AT-S63 Main Menu:

```
menu
```

Equivalent Command

```
exit
```

For information, see "EXIT" on page 33.

SAVE CONFIGURATION

Syntax

```
save configuration
```

Parameters

None.

Description

This command saves your changes to the switch's active boot configuration file for permanent storage.

Whenever you make a change to an operating parameter of the switch, such as enter a new IP address or create a new VLAN, the change is stored in temporary memory. It will be lost the next time you reset the switch or power cycle the unit.

To permanently save your changes, you must use this command. The changes are saved in the active boot configuration file as a series of commands. The commands in the file are used by the switch to recreate all of its settings, such as VLANs and port settings, whenever you reset or power cycle the unit.

To view the name of the currently active boot configuration file, see "SHOW CONFIG" on page 222. To view the contents of a configuration file, see "SHOW FILE" on page 223. For background information on boot configuration files, refer to Chapter 11, "File System" in the *AT-S63 Management Software Menus Interface User's Guide*.

Example

The following command saves your configuration changes to the active boot configuration file:

```
save configuration
```

SET PROMPT

Syntax

`set prompt="`*`prompt`*`"`

Parameter

prompt	Specifies the command line prompt. The prompt can be from one to 12 alphanumeric characters. Spaces and special characters are allowed. The prompt must be enclosed in quotes.

Description

This command changes the command prompt. Assigning each switch a different command prompt can make it easier for you to identify the different switches in your network when you manage them.

Note
If you define the system name before you set up a system prompt, the switch uses the first 16 characters of the system name as the prompt. See “SET SYSTEM” on page 64.

Example

The following command changes the command prompt to “Sales Switch”:

```
set prompt="Sales Switch"
```

Equivalent Command

`set asyn prompt="`*`prompt`*`"`

For information, see “SET ASYN” on page 57.

SET SWITCH CONSOLEMODE

Syntax

```
set switch consolemode=menu|cli
```

Parameter

consolemode — Specifies the mode you want management sessions to start in. Options are:

- menu — Specifies the AT-S63 Main Menu.
- cli — Specifies the command line prompt. This is the default.

Description

You use this command to specify whether you want your management sessions to start by displaying the command line interface (CLI) or the AT-S63 Main Menu. The default is the CLI.

Example

The following command configures the management software to display the menus whenever you start a management session:

```
set switch consolemode=menu
```

SHOW USER

Syntax

```
show user
```

Parameter

None.

Description

Displays the user account you used to log on to manage the switch.

Example

```
show user
```

Chapter 3

Basic Switch Commands

This chapter contains the following commands:

- “DISABLE DHCPBOOTP” on page 43
- “DISABLE IP REMOTEASSIGN” on page 44
- “DISABLE TELNET” on page 45
- “ENABLE BOOTP” on page 46
- “ENABLE DHCP” on page 47
- “ENABLE IP REMOTEASSIGN” on page 48
- “ENABLE TELNET” on page 49
- “PING” on page 50
- “PURGE IP” on page 51
- “RESET SWITCH” on page 52
- “RESET SYSTEM” on page 53
- “RESTART REBOOT” on page 54
- “RESTART SWITCH” on page 55
- “SET ASYN” on page 57
- “SET IP INTERFACE” on page 58
- “SET IP ROUTE” on page 60
- “SET PASSWORD MANAGER” on page 61
- “SET PASSWORD OPERATOR” on page 62
- “SET SWITCH CONSOLETIMER” on page 63
- “SET SYSTEM” on page 64
- “SET TELNET INSERTNULL” on page 65
- “SET USER PASSWORD” on page 66
- “SHOW ASYN” on page 67
- “SHOW CONFIG DYNAMIC” on page 68
- “SHOW CONFIG INFO” on page 71
- “SHOW DHCPBOOTP” on page 72
- “SHOW IP INTERFACE” on page 74
- “SHOW IP ROUTE” on page 75
- “SHOW SWITCH” on page 76

- “SHOW SYSTEM” on page 79

Note
Remember to save your changes with the SAVE CONFIGURATION command.

DISABLE DHCPBOOTP

Syntax

```
disable dhcpbootp
```

Parameters

None.

Description

This command deactivates the DHCP and BOOTP client software on the switch. The default setting for the DHCP and BOOTP client software is disabled.

To activate the DHCP or BOOTP client software, refer to "ENABLE BOOTP" on page 46, "ENABLE DHCP" on page 47, "ENABLE IP REMOTEASSIGN" on page 48, or "SET IP INTERFACE" on page 58.

Example

The following command deactivates the DHCP and BOOTP client software:

```
disable dhcpbootp
```

Equivalent Command

```
disable ip remoteassign
```

For information, see "DISABLE IP REMOTEASSIGN" on page 44.

DISABLE IP REMOTEASSIGN

Syntax

```
disable ip remoteassign
```

Parameters

None.

Description

This command deactivates the DHCP and BOOTP client software on the switch. The default setting for the DHCP and BOOTP client software is disabled.

To activate the DHCP or BOOTP client software, refer to “ENABLE BOOTP” on page 46, “ENABLE DHCP” on page 47, “ENABLE IP REMOTEASSIGN” on page 48, or “SET IP INTERFACE” on page 58.

Example

The following command deactivates the DHCP and BOOTP client software:

```
disable ip remoteassign
```

Equivalent Command

```
disable dhcpbootp
```

For information, see “DISABLE DHCPBOOTP” on page 43.

DISABLE TELNET

Syntax

```
disable telnet
```

Parameters

None.

Description

This command disables the Telnet server software on the switch. You can disable the server software if you do not want anyone to manage the switch using the Telnet application protocol or if you plan to use the Secure Shell protocol. The default setting for the Telnet server is enabled.

Example

The following command deactivates the Telnet server:

```
disable telnet
```

ENABLE BOOTP

Syntax

```
enable bootp
```

Parameters

None.

Description

This command activates the BOOTP client software on the switch. The default setting for the BOOTP client software is disabled. When activating the BOOTP client software, note the following:

- The switch immediately begins to query the network for a BOOTP server after the command is entered. The switch continues to query the network for its IP configuration until it receives a response.
- Any static IP address, subnet mask, or gateway address assigned to the switch is replaced with the value the switch receives from the BOOTP server. If you later disable BOOTP, these values are returned to their default settings.
- To disable BOOTP, refer to “DISABLE DHCPBOOTP” on page 43 or “DISABLE IP REMOTEASSIGN” on page 44.
- You cannot manually assign an IP address or subnet mask to a switch when the BOOTP client software has been activated.
- The switch does not support running both the BOOTP client software and DHCP client software at the same time. To have the switch obtain its IP configuration from a DHCP server instead of a BOOTP server, activate the DHCP client software on the switch using “ENABLE DHCP” on page 47 or “SET IP INTERFACE” on page 58.

Example

The following command activates the BOOTP client software on the switch:

```
enable bootp
```

Equivalent Command

```
set ip interface=eth0 ipaddress=bootp
```

For information, see “SET IP INTERFACE” on page 58.

ENABLE DHCP

Syntax

```
enable dhcp
```

Parameters

None.

Description

This command activates the DHCP client software on the switch. The default setting for the DHCP client software is disabled. When activating the DHCP client software, note the following:

- The switch immediately begins to query the network for a DHCP server after the command is entered. The switch continues to query the network for its IP configuration until it receives a response.
- Any static IP address, subnet mask, or gateway address assigned to the switch is replaced with the value the switch receives from the DHCP server. If you later disable DHCP, these values are returned to their default settings.
- To disable DHCP, refer to "DISABLE DHCPBOOTP" on page 43 or "DISABLE IP REMOTEASSIGN" on page 44.
- You cannot manually assign an IP address or subnet mask to a switch when the DHCP client software has been activated.
- The switch does not support running both the BOOTP client software and DHCP client software at the same time. To have the switch obtain its IP configuration from a BOOTP server instead of a DHCP server, activate the BOOTP client software on the switch using "ENABLE BOOTP" on page 46 or "SET IP INTERFACE" on page 58.

Example

The following command activates the DHCP client software on the switch:

```
enable dhcp
```

Equivalent Commands

```
enable ip remoteassign
```

For information, see "ENABLE IP REMOTEASSIGN" on page 48.

```
set ip interface=eth0 ipaddress=dhcp
```

For information, see "SET IP INTERFACE" on page 58.

ENABLE IP REMOTEASSIGN

Syntax

```
enable ip remoteassign
```

Parameters

None.

Description

This command activates the DHCP client software on the switch. The default setting for the DHCP client software is disabled. When activating the DHCP client software, note the following:

- The switch immediately begins to query the network for a DHCP server after the command is entered. The switch continues to query the network for its IP configuration until it receives a response.
- Any static IP address, subnet mask, or gateway address assigned to the switch is replaced with the value the switch receives from the DHCP server. If you later disable DHCP, these values are returned to their default settings.
- To disable DHCP, refer to “DISABLE DHCPBOOTP” on page 43 or “DISABLE IP REMOTEASSIGN” on page 44.
- You cannot manually assign an IP address or subnet mask to a switch when the DHCP client software has been activated.
- The switch does not support running both the BOOTP client software and DHCP client software at the same time. To have the switch obtain its IP configuration from a BOOTP server instead of a DHCP server, activate the BOOTP client software on the switch using “ENABLE BOOTP” on page 46 or “SET IP INTERFACE” on page 58.

Example

The following command activates the DHCP client software on the switch:

```
enable ip remoteassign
```

Equivalent Commands

```
enable dhcp
```

For information, see “ENABLE DHCP” on page 47.

```
set ip interface=eth0 ipaddress=dhcp
```

For information, see “SET IP INTERFACE” on page 58.

ENABLE TELNET

Syntax

```
enable telnet
```

Parameters

None.

Description

This command activates the Telnet server on the switch. With the server activated, you can manage the switch using the Telnet application protocol from any management station on your network. To disable the server, refer to "DISABLE TELNET" on page 45. The default setting for the Telnet server is enabled.

Example

The following command activates the Telnet server:

```
enable telnet
```

PING

Syntax

`ping` *`ipaddress`*

Parameter

ipaddress	Specifies the IP address of an end node you want the switch to ping.

Description

This command instructs the switch to ping an end node. You can use this command to determine whether a valid link exists between the switch and another device.

> **Note**
> The switch must have an IP address and subnet mask for this command.

Example

The following command pings an end node with the IP address of 149.245.22.22

```
ping 149.245.22.22
```

The results of the ping are displayed on the screen.

PURGE IP

Syntax

```
purge ip [ipaddress] [netmask] [route]
```

Parameters

ipaddress	Returns the switch's IP address to the default setting 0.0.0.0.
netmask	Returns the subnet mask to the default setting 0.0.0.0.
route	Returns the gateway address to the default setting 0.0.0.0.

Description

This command returns the switch's IP address, subnet mask, and default gateway address to the default settings.

To set these parameters, refer to "SET IP INTERFACE" on page 58 and "SET IP ROUTE" on page 60. To view the current settings, refer to "SET SYSTEM" on page 64.

Examples

The following command returns the IP address and subnet mask to the default values:

```
purge ip ipaddress netmask
```

The following command resets just the gateway address to its default value:

```
purge ip route
```

The following command resets all three parameters:

```
purge ip
```

RESET SWITCH

Syntax

```
reset switch
```

Parameters

None.

Description

This command does the following:

- Performs a soft reset on all ports. The reset takes less than a second to complete. The ports retain their current operating parameter settings. To perform this function on a per-port basis, refer to “RESET SWITCH PORT” on page 130.
- Resets the statistics counters for all ports to zero. To perform this function on a per-port basis, refer to “RESET SWITCH PORT COUNTER” on page 150.
- Deletes all dynamic MAC addresses from the MAC address table. To perform this function on a per-port basis, refer to “RESET SWITCH FDB” on page 160.

Example

This command resets the switch according to the description above:

```
reset switch
```

RESET SYSTEM

Syntax

```
reset system [name] [contact] [location]
```

Parameters

name	Deletes the switch's name.
contact	Deletes the switch's contact.
location	Deletes the switch's location.

Description

This command delete's the switch's name, the name of the network administrator responsible for managing the unit, and the location of the unit. To set these parameters, refer to "SET SYSTEM" on page 64. To view the current settings, refer to "SHOW SYSTEM" on page 79.

Examples

This command deletes all three parameter settings:

```
reset system
```

This command deletes just the name:

```
reset system name
```

RESTART REBOOT

Syntax

```
restart reboot
```

Parameters

None.

Description

This command resets the switch. The switch runs its internal diagnostics, loads the AT-S63 management software, and configures its parameter settings using the active boot configuration file. The reset can take from 20 seconds to two minutes to complete, depending on the number and complexity of the commands in the active boot configuration file. The switch does not forward traffic during the reset process. Some network traffic may be lost.

> **Note**
> Be sure to use the SAVE CONFIGURATION command to save your changes before resetting the switch. Any unsaved changes are lost.

Your local or remote management session with the switch ends when the unit is reset. You must reestablish the session to continue managing the unit.

Example

The following resets the switch:

```
restart reboot
```

RESTART SWITCH

Syntax

```
restart switch config=none|filename.cfg
```

Parameters

config — Specifies the configuration file. The file must already exist on the switch. The NONE option returns the switch to its default values.

Description

This command loads a different configuration file on the switch or returns the switch's parameter settings to their default values. This command can also be used to reset the switch.

If you specify a configuration file, the switch automatically resets itself and configures its parameters according to the settings in the configuration file specified in the command.

Specifying the NONE option returns the switch's operating parameters to the default setting. Please note the following before using this option:

- Returning the switch to its default values deletes all port-based and tagged VLANs you may have created on the switch.
- This option does not delete files from the AT-S63 file system. To delete files, refer to "DELETE FILE" on page 213.
- This option does not delete encryption keys stored in the key database. To delete encryption keys, refer to "DESTROY ENCO KEY" on page 618.
- Returning a switch to its default values does not change the settings in the active boot configuration file.
- To reset the active configuration file back to the default settings, you must use the SAVE CONFIGURATION command after the switch reboots and you have reestablished your management session. Otherwise, the switch reverts to the previous configuration the next time you reset the switch.

Note
The switch does not forward network traffic during the reset process. Some network traffic may be lost.

Note
For a list of default values, refer to Appendix A, “AT-S63 Default Settings” in the *AT-S63 Management Software Menus Interface User’s Guide*.

This command does not change the assignment of the active boot configuration file, the configuration file the switch uses the next time it is reset. If you reset or power cycle the switch, the switch uses the previous configuration. To change the active boot configuration file, refer to “SET CONFIG” on page 219.

Your local or remote management session with the switch ends when you reset the switch. You must reestablish the session to continue managing the switch.

Examples

The following command configures the switch using the configuration file named `switch12.cfg`:

```
restart switch config=switch12.cfg
```

The following command resets the switch to its default values:

```
restart switch config=none
```

The following command resets the switch:

```
restart switch
```

Equivalent Command

```
restart reboot
```

For information, see “RESTART REBOOT” on page 54.

SET ASYN

Syntax

```
set asyn [speed=1200|2400|4800|9600|19200|38400|
57600|115200] [prompt="prompt"]
```

Parameters

speed	Sets the speed (baud rate) of the serial terminal port on the switch. The default is 9600 bps.
prompt	Specifies the command line prompt. The prompt can be from one to 12 alphanumeric characters. Spaces and special characters are allowed. The prompt must be enclosed in double quotes. This parameter performs the same function as "SET PROMPT" on page 38.

Description

This command sets the baud rate of the serial terminal port on the switch. The port is used for local management of the switch. You can also use this command to set the command line prompt.

Note
A change to the baud rate of the port ends your management session if you are managing the switch locally. To reestablish a local management session you must change the speed of the terminal or the terminal emulator program to match the new speed of the serial terminal port on the switch.

Example

The following command sets the baud rate to 115200 bps:

```
set asyn speed=115200
```

Equivalent Command

```
set prompt="prompt"
```

For information, see "SET PROMPT" on page 38.

SET IP INTERFACE

Syntax

```
set ip interface=eth0 ipaddress=ipaddress|bootp|dhcp
mask|netmask=subnetmask
```

Parameters

interface	Specifies the interface number. This value is always eth0.
ipaddress	Specifies an IP address for the switch or activates the BOOTP or DHCP client software.
mask ***or*** netmask	Specifies the subnet mask for the switch. You must specify a subnet mask when you manually assign the switch an IP address. These parameters are equivalent. The default is 0.0.0.0.

Description

This command configures the following switch parameters:

- IP address
- Subnet mask

This command can also activate the DHCP or BOOTP client software on the switch. If you are using this command to activate the client software, note the following:

- The switch immediately begins to query the network for a BOOTP or DHCP server after the command is entered. The switch continues to query the network for its IP configuration until it receives a response.
- Any static IP address, subnet mask, or gateway address assigned to the switch is replaced with the value the switch receives from the BOOTP or DHCP server. If you later disable BOOTP or DCHP, these values are returned to their default settings.
- You cannot manually assign an IP address or subnet mask to a switch when the BOOTP or DHCP client software has been activated.
- The switch does not support running both the BOOTP client software and DHCP client software at the same time.

To display the current IP address and subnet mask, refer to “SHOW IP INTERFACE” on page 74. To return the IP address and subnet mask to their default values, refer to “PURGE IP” on page 51.

Examples

The following command sets the switch's IP address to 140.35.22.22 and the subnet mask to 255.255.255.0:

```
set ip interface=eth0 ipaddress=140.35.22.22
netmask=255.255.255.0
```

The following command sets just the subnet mask:

```
set ip interface=eth0 netmask=255.255.255.252
```

The following command activates the DHCP client software:

```
set ip interface=eth0 ipaddress=dhcp
```

Equivalent Commands

```
enable bootp
```

For information, refer to "ENABLE BOOTP" on page 46

```
enable dhcp
```

For information, refer to "ENABLE DHCP" on page 47.

```
enable ip remoteassign
```

For information, refer to "ENABLE IP REMOTEASSIGN" on page 48.

```
set ip interface=eth0 ipaddress=bootp
```

```
set ip interface=eth0 ipaddress=dhcp
```

For information, refer to "SET IP INTERFACE" on page 58.

SET IP ROUTE

Syntax

```
set ip route ipaddress=ipaddress
```

Parameter

ipaddress	Specifies the IP address of the default gateway for the switch.

Description

This command specifies the IP address of the default gateway for the switch. This IP address is required if you intend to remotely manage the device from a remote management station that is separated from the unit by a router. To display the current gateway address, refer to “SHOW IP INTERFACE” on page 74.

Example

The following command sets the default gateway to 140.35.22.12:

```
set ip route ipaddress=140.35.22.12
```

SET PASSWORD MANAGER

Syntax

```
set password manager
```

Parameters

None.

Description

This command sets the manager's password. The manager account allows you to view and change all switch parameters. The default password is "friend." The password can be from 0 to 16 alphanumeric characters. Allied Telesyn recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

Example

The following command changes the manager's password:

```
set password manager
```

Follow the prompts to enter the new password.

Equivalent Command

```
set user manager password=password
```

For information, see "SET USER PASSWORD" on page 66.

SET PASSWORD OPERATOR

Syntax

```
set password operator
```

Parameters

None.

Description

This command sets the operator's password. Logging in as operator allows you to only view the switch parameters. The default password is "operator." The password can be from 0 to 16 alphanumeric characters. Allied Telesyn recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

Example

The following command changes the operator's password:

```
set password operator
```

Follow the prompts to enter the new password.

Equivalent Command

```
set user operator password=password
```

For information, see "SET USER PASSWORD" on page 66.

SET SWITCH CONSOLETIMER

Syntax

```
set switch consoletimer=value
```

Parameter

consoletimer — Specifies the console timer in minutes. The range is 1 to 60 minutes. The default is 10 minutes.

Description

This command sets the console timer, which is used by the management software to end inactive management sessions. If the AT-S63 software does not detect any activity from a local or remote management station after the period of time set by the console timer, it automatically ends the management session. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. To view the current console timer setting, refer to "SHOW SWITCH" on page 76.

Example

The following command sets the console timer to 25 minutes:

```
set switch consoletimer=25
```

SET SYSTEM

Syntax

```
set system [name="name"] [contact="contact"]
[location="location"]
```

Parameters

name	Specifies the name of the switch. The name can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes (“ “). Spaces are allowed.
contact	Specifies the name of the network administrator responsible for managing the switch. The contact can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes. Spaces are allowed.
location	Specifies the location of the switch. The location can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes. Spaces are allowed.

Description

This command sets a switch’s name, the name of the network administrator responsible for managing the unit, and the location of the unit.

If a parameter already has a value, the new value replaces the existing value. To view the current values for these parameters, refer to “SHOW SYSTEM” on page 79. To delete a value without assigning a new value, refer to “RESET SYSTEM” on page 53.

Note
If you define the system name before you set up a system prompt, the switch uses the first 16 characters of the system name as the prompt. See “SET PROMPT” on page 38.

Examples

The following command sets a switch’s information:

```
set system name="Sales" contact="Jane Smith" location="Bldg
3, rm 212"
```

The following command sets just the system’s name:

```
set system name="PR Office"
```

SET TELNET INSERTNULL

Syntax

```
set telnet insertnull=on|off
```

Parameters

insertnull — Controls whether a NULL character is inserted after each CR sent by the Telnet server to the remote client. Options are:

- on — Sends a NULL character after each CR sent to the remote client.
- off — Specifies that no NULL character is sent to the remote client. This is the default setting.

Description

You can use this command to toggle the Telnet server on the switch to add a NULL character after each CR for those Telnet clients that require the character in order to display the information correctly. The default setting on the switch is to not send the NULL character after a CR. To view the current setting, see "SHOW SWITCH" on page 76.

Example

This command configures the switch to send a NULL character after each CR during a Telnet management session:

```
set telnet insertnull=on
```

SET USER PASSWORD

Syntax

`set user manager|operator password=`*`password`*

Parameter

password Specifies the password.

Description

This command sets the manager or operator's password. The default manager password is "friend." The default operator password is "operator." The password can be from 0 to 16 alphanumeric characters. Allied Telesyn recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

Example

The following command sets the operator's password to "newby":

```
set user operator password=newby
```

Equivalent Commands

`set password manager`

For information, see "SET PASSWORD MANAGER" on page 61

`set password operator`

For information, see "SET PASSWORD OPERATOR" on page 62

SHOW ASYN

Syntax

```
show asyn
```

Parameters

None.

Description

This command displays the settings for the serial terminal port on the switch, used for local management of the device. An example of the display is shown in Figure 1.

```
Asynchronous Port (Console) Information:
     Baud Rate ................................ 115200
     Parity ................................... NONE
     Data bits ................................ 8
     Stop bits ................................ 1
     Prompt ................................... "Sales Switch"
```

Figure 1. SHOW ASYN Command

To configure the serial port's baud rate, refer to "SET ASYN" on page 57. To configure the command line prompt, refer to "SET PROMPT" on page 38. You cannot adjust the parity, data bits, or stop bit of the serial terminal port.

Example

The following command displays the serial terminal port settings:

```
show asyn
```

SHOW CONFIG DYNAMIC

Syntax

```
show config dynamic[=module]
```

Parameters

module — Displays the settings of a particular switch module. You can specify only one module at a time. For a list of modules, refer to Table 3.

Description

This command displays the settings of the switch parameters that have been changed from their default values, including those not yet saved to the active boot configuration file. The parameters are displayed in their command line command equivalents. You can view all of the settings or limit the display to just those of a particular switch module. An example of the display is shown in Figure 2.

```
---Start of current configuration ------------------

#
# System Configuration
#
set system name="Production Server"
set system contact="Jane Smith"
set system location="Bldg. 2, room 411"

#
# IP Configuration
#
```

Figure 2. SHOW CONFIG DYNAMIC Command

The MODULE variable is used to limit the display to the parameter settings of a particular switch module. You can specify only one module per command. The modules are listed in Table 3.

Table 3. Module Variable

Variable	Description
ACL	Port access control list
AUTH	Manager and operator passwords (encrypted) and RADIUS and TACACS+

Table 3. Module Variable (Continued)

Variable	Description
CLASSIFIER	Classifiers for ACL and QoS
DOS	Denial of service defense
ENCO	Encryption keys
ENHSTACK	Enhanced stacking
EVTLOG	Event log and syslog client
GARP	GARP and GVRP
IGMPSNOOP	IGMP snooping
IP	System IP configuration, DHCP, and BOOTP
LACP	Link Aggregation Control Protocol
MAC	Static MAC addresses
MACTIMER	MAC address table timeout value
MACVLAN	MAC address-based VLANs
MGMTACL	Management access control list
MIRROR	Source ports of port mirror
MIRTO	Destination port of port mirror
MLDSNOOP	MLD snooping
PKI	Public Key Infrastructure
PORT	Port configuration
PORTACC	802.1x port-based access control
PORTSEC	MAC address-based port security
PORTTRUNK	Static port trunking
QOS	Quality of Service
RRPSNOOP	RRP snooping
SNMP	SNMP
SNTP	SNTP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols

Table 3. Module Variable (Continued)

Variable	Description
STP1	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SWITCH	Switch console timer, console startup mode, serial port baud rate, Telnet server
SYSTEM	Administrator name, switch name, and switch location
VLAN	Port-based and tagged VLANs, and multiple VLAN modes

Examples

The following command displays all the switch parameter settings that have been changed from their default values:

```
show config dynamic
```

The following command displays the non-default parameter settings for IGMP snooping:

```
show config dynamic=igmpsnoop
```

SHOW CONFIG INFO

Syntax

```
show config info
```

Parameters

None.

Description

This command displays the settings of all the switch parameters, including those not yet saved to the active boot configuration file.

Examples

The following command displays all the parameter settings on the switch:

```
show config info
```

SHOW DHCPBOOTP

Syntax

```
show dhcpbootp
```

Parameters

None.

Description

This command displays the status of the DHCP and BOOTP client software on the switch. If neither is activated on the switch, the command displays the message in Figure 3.

```
DHCP/BOOTP Information:
   Status ............................. DISABLE
```

Figure 3. SHOW DHCPBOOTP Command

If DHCP is activated, the command displays the prompt in Figure 4.

```
DHCP/BOOTP Information:
   Status ............................. DHCP
```

Figure 4. SHOW DHCPBOOTP Command - DHCP Activated

If BOOTP is activated on the switch, the command displays the prompt in Figure 5.

```
DHCP/BOOTP Information:
   Status ............................. BOOTP
```

Figure 5. SHOW DHCPBOOTP Command - BOOTP Activated

DHCP and BOOTP cannot both be active on a switch at the same time.

The default setting for the DHCP and BOOTP client software is disabled.

To enable the DHCP or BOOTP client software, refer to “ENABLE BOOTP” on page 46, “ENABLE DHCP” on page 47, “SET IP INTERFACE” on page 58, or “ENABLE IP REMOTEASSIGN” on page 48. To disable the client software, refer to “DISABLE DHCPBOOTP” on page 43 or “DISABLE IP REMOTEASSIGN” on page 44.

Example

The following command displays the status of the DHCP and BOOTP client software:

```
show dhcpbootp
```

SHOW IP INTERFACE

Syntax

```
show ip interface=eth0
```

Parameter

interface	Specifies the switch's interface number. This value is always eth0.

Description

This command displays the IP address, subnet mask, and default gateway address of the switch. Figure 6 is an example of the information displayed by this command.

```
IP Interface Information:
 IP Address ......................... 149.44.44.44
 Net Mask ........................... 255.255.255.0
 Default Route ...................... 0.0.0.0
```

Figure 6. SHOW IP INTERFACE Command

To manually set the IP address and subnet mask, refer to "SET IP INTERFACE" on page 58. To manually set the default gateway address, refer to "SET IP ROUTE" on page 60. To enable the DHCP or BOOTP client software, refer to "ENABLE BOOTP" on page 46, "ENABLE DHCP" on page 47, "SET IP INTERFACE" on page 58, or "ENABLE IP REMOTEASSIGN" on page 48.

Example

The following command displays the IP address, subnet mask, and default gateway of the switch:

```
show ip interface=eth0
```

Equivalent Command

```
show ip route
```

This command displays just the default gateway address. For information, refer to "SHOW IP ROUTE" on page 75.

SHOW IP ROUTE

Syntax

```
show ip route
```

Parameters

None.

Description

This command displays the switch's default gateway address. To manually set the default gateway address, refer to "SET IP ROUTE" on page 60.

Example

The following command displays the default gateway address of the switch:

```
show ip route
```

Equivalent Command

```
show ip interface=eth0
```

This command displays the switch's IP address and subnet mask in addition to the default gateway address. For information, refer to "SHOW IP INTERFACE" on page 74.

SHOW SWITCH

Syntax

```
show switch
```

Parameters

None.

Description

This command displays a variety of switch parameters. An example of the display is shown in Figure 7.

```
Switch Information:

Application Software Version ......... ATS63 v1.2.0 NE
Application Software Build Date ...... Jun 10 2005 16:27:38
Bootloader Version ................... ATS63_LOADER v1.3.0
Bootloader Build Date ................ Apr  7 2005 16:25:19
MAC Address .......................... 00:21:46:A7:B4:43
VLAN Mode ............................ User Configured
Management VLAN ...................... 1 (Default_VLAN)
Ingress Filtering .................... OFF
Active Spanning Tree version ......... RSTP
Mirroring State ...................... Disabled
Enhanced Stacking mode ............... Master
Console Disconnect Timer Interval .... 10 minute(s)
Web Server Status .................... Enabled
Telnet Server status ................. Enabled
Telnet insert NULL ................... OFF
MAC address aging time ............... 300 second(s)
Console Startup Mode ................. CLI
Multicast Mode ....................... Forward Across VLANs
```

Figure 7. SHOW SWITCH Command

This command displays the following information:

- Application software version and Application software build date - The version number and build date of the AT-S63 management software.
- Bootloader version and Bootloader build date - The version number and build date of the AT-S63 bootloader.
- MAC address - The MAC address of the switch. This value cannot be changed.

- VLAN mode - The switch's VLAN mode. The three possible VLAN modes are:
  - User configured (for creating your own port-based and tagged VLANs)
  - 802.1Q-compliant
  - Non-802.1Q-compliant.

  The default is user configured. To set a switch's VLAN mode, refer to "SET SWITCH VLANMODE" on page 526.
- Management VLAN - The ID number of the management VLAN. The switch uses the management VLAN for remote Telnet, SSH, and web browser management sessions. The default is 1, which is the ID number for the Default_VLAN. To set the management VLAN, refer to "SET SWITCH MANAGEMENTVLAN" on page 525.
- Ingress filtering - The status of ingress filtering on the switch. When ingress filtering is activated, tagged frames are filtered when they are received on a port. When ingress filtering is deactivated, which is the default, tagged frames are filtered before they are transmitted out a port. To set ingress filtering, refer to "SET SWITCH INFILTERING" on page 524.
- Active Spanning Tree version - The spanning tree protocol that has been designated as the active protocol on the switch. To configure or enable a spanning tree protocol, you must first designate it as the active protocol on the switch. The switch supports, STP, RSTP, and MSTP. The default is RSTP. To select an active spanning tree protocol, refer to "ACTIVATE STP" on page 462, "ACTIVATE RSTP" on page 476, and "ACTIVATE MSTP" on page 490.
- Mirroring state - The status of port mirroring. The display includes the destination port as well as the ingress and egress source ports if port mirroring is activated on the switch. To configure port mirroring, refer to "SET SWITCH MIRROR" on page 194 and "SET SWITCH PORT MIRROR" on page 195.
- Enhanced stacking mode - The enhanced stacking mode of the switch, which can be master, slave, or unavailable. The default is slave. To set the enhanced stacking status, refer to "SET SWITCH STACKMODE" on page 84.
- Console disconnect timer interval - The current value of the console timer, used by the management software to end inactive management sessions. The AT-S63 software ends a local or remote management session if it does not detect any management activity for the length of time specified by the console timer. The default is 10 minutes. To set the console timer, refer to "SET SWITCH CONSOLETIMER" on page 63.
- Web server status - The status of the web server. When the web server is disabled, you cannot remotely manage the switch using a web browser and the web browser interface. The default setting is enabled.

To enable or disable the server, refer to “ENABLE HTTP SERVER” on page 605 and “DISABLE HTTP SERVER” on page 604.

- Telnet server status - The status of the Telnet server. When the Telnet server is disabled, you cannot remotely manage the switch using the Telnet application protocol. The default setting is enabled. To enable or disable the server, refer to “ENABLE TELNET” on page 49 and “DISABLE TELNET” on page 45.
- Telnet insert NULL - The status of the Telnet NULL parameter. When ON, the Telnet server on the switch adds a NULL character after each CR for those Telnet clients that require the character to display the information correctly. When OFF, the default setting, no NULL character is set after a CR. To set this feature, see “SET TELNET INSERTNULL” on page 65.
- MAC address aging time - The current value for the MAC address aging timer. The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. To set this value, refer to “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 161.
- Console startup mode - The management interface —menus or command line — that initially appears when you start a local or remote management session. The default is the command line interface. To set the startup mode, refer to “SET SWITCH CONSOLEMODE” on page 39.
- Multicast Mode - The multicast mode, which determines the behavior of the switch when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets To set the multicast mode, refer to “SET SWITCH MULTICASTMODE” on page 471.

Example

The following command displays the switch information described above:

```
show switch
```

SHOW SYSTEM

Syntax

```
show system
```

Parameters

None.

Description

This command displays the following information:

- MAC address
- IP address
- Model name
- Subnet mask
- Serial number
- Gateway address
- System up time
- Bootloader version
- Bootloader build date
- Application software version
- Application software build date
- System name
- Administrator (the network administrator responsible for managing the unit)
- Location (of the unit)
- System 1.25 V power
- System 1.8 V power
- System 2.5 V power
- System 3.3 V power
- System 5 V power
- System 12 V power
- System temperature
- System fan speed
- Main PSU
- RPS

For instructions on how to set the name, contact, and location of the switch, see “SET SYSTEM” on page 64.

Example

The following command displays the information about the switch:

```
show system
```

Chapter 4

Enhanced Stacking Commands

This chapter contains the following commands:

- “ACCESS SWITCH” on page 82
- “SET SWITCH STACKMODE” on page 84
- “SHOW REMOTELIST” on page 86

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 4, “Enhanced Stacking” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ACCESS SWITCH

Syntax

```
access switch number=number|macaddress=macaddress
```

Parameters

number	Specifies the number of the switch in an enhanced stack that you want to manage. You view this number using the SHOW REMOTELIST command.
macaddress	Specifies the MAC address of the switch you want to manage. This can also be displayed using the SHOW REMOTELIST command. You can enter the address in either of the following formats: xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

Description

This command starts a management session on another switch that supports enhanced stacking, such as another AT-9400 Series switch or an AT-8000 Series switch. You can specify the switch by switch number or by MAC address, both of which are displayed with “SHOW REMOTELIST” on page 86.

Note
You must perform the ACCESS SWITCH command from a management session of a master switch. This command will not work from a management session of a slave switch. To determine the master or slave status of your switch, use “SHOW SWITCH” on page 76.

Note
You must perform the SHOW REMOTELIST command before using the ACCESS SWITCH command.

When you are finished managing a slave switch, use the LOGOFF, LOGOUT, or QUIT command to end the management session and return back to the master switch from which you started the management session. For information, refer to “LOGOFF, LOGOUT and QUIT” on page 35.

Examples

The following command starts a management session on switch number 12:

```
access switch number=12
```

The following command starts a management session on a switch with the MAC address 00:30:84:52:02:11

```
access switch macaddress=003084520211
```

SET SWITCH STACKMODE

Syntax

```
set switch stackmode=master|slave|unavailable
```

Parameter

stackmode	Specifies the enhanced stacking mode of the switch. The options are:	
	master	Specifies the switch's stacking mode as master. A master switch must be assigned an IP address and subnet mask.
	slave	Specifies the switch's stacking mode as slave. A slave does not need an IP address. This is the default setting for a switch.
	unavailable	Specifies the switch's stacking mode as unavailable. A switch with this status cannot be managed from an enhanced stack. It can be managed locally through its RS-232 terminal port or remotely if it is assigned an IP address and subnet mask.

Description

This command sets a switch's enhanced stacking status.

Note
To determine the master or slave status of a switch, use "SHOW SWITCH" on page 76.

Note
You cannot change the stacking status of a switch through enhanced stacking. If a switch does not have an IP address or subnet mask, such as a slave switch, you must use a local management session to change its stacking status. If the switch has an IP address and subnet mask, such as a master switch, you can use either a local or a Telnet management session to change its stacking status.

Example

The following command sets the switch's stacking status to master:

```
set switch stackmode=master
```

SHOW REMOTELIST

Syntax

```
show remotelist [sorted by=macaddress|name]
```

Parameter

sorted	Sorts the list either by MAC address or by name. The default is by MAC address.

Description

This command displays the list of switches in an enhanced stack. The list does not include the master switch where you started the management session or switches with a stacking status of unavailable.

> **Note**
> You must perform the SHOW REMOTELIST command from the management session of the master switch where you started the management session. This command will not work from a slave switch. Nor will the command work from a master switch that you accessed through enhanced stacking from another master switch. To determine the master or slave status of your switch, use “SHOW SWITCH” on page 76.

An example of the information displayed by this command is shown in Figure 8.

```
Searching for slave devices. Please wait...

Num   MAC Address        Name           Switch   Software     Switch
                                        Mode     Version      Model
-------------------------------------------------------------------------
01    00:21:46:A7:B4:04  Production..   Slave    S63 v1.2.0   AT-9424T/SP
02    00:21:46:A7:B4:43  Marketing      Slave    S63 v1.2.0   AT-9424T/SP
03    00:30:84:00:00:02  Tech Suppo..   Slave    S62 v1.3.0   AT-8524M
```

Figure 8. SHOW REMOTELIST Command

Examples

The following command displays the switches in an enhanced stack, sorted by MAC address, the default sorting method:

```
show remotelist
```

The following command displays the switches sorted by name:

```
show remotelist sorted by=name
```

Chapter 5

Simple Network Time Protocol (SNTP) Commands

This chapter contains the following commands:

- “ADD SNTPSERVER PEER|IPADDRESS” on page 90
- “DELETE SNTPSERVER PEER|IPADDRESS” on page 91
- “DISABLE SNTP” on page 92
- “ENABLE SNTP” on page 93
- “PURGE SNTP” on page 94
- “SET DATE” on page 95
- “SET SNTP” on page 96
- “SET TIME” on page 97
- “SHOW SNTP” on page 98
- “SHOW TIME” on page 100

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on SNTP, refer to Chapter 3, “Basic Switch Parameters” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD SNTPSERVER PEER|IPADDRESS

Syntax

```
add sntpserver peer|ipaddress=ipaddress
```

Parameter

peer ***or*** ipaddress	Specifies the IP address of an SNTP server. These parameters are equivalent.

Description

This command adds the IP address of an SNTP server to the SNTP client software on the switch. The switch uses the SNTP server to set its date and time. If an IP address has already been assigned, the new address overwrites the old address.

> **Note**
> If the switch is obtaining its IP address and subnet mask from a DHCP sever, you can configure the DHCP server to provide the switch with an IP address of an NTP or SNTP server. If you configured the DHCP server to provide this address, then you do not need to enter it with this command.

Example

The following command specifies the IP address of 148.35.16.248 for the SNTP server:

```
add sntpserver ipaddress=148.35.16.248
```

DELETE SNTPSERVER PEER|IPADDRESS

Syntax

```
delete sntpserver peer|ipaddress=ipaddress
```

Parameter

peer ***or*** ipaddress	Specifies the IP address of an SNTP server. The parameters are equivalent.

Description

This command deletes the IP address of the SNTP server from the SNTP client software on the switch and returns the parameter to the default value of 0.0.0.0. To view the IP address, refer to "SHOW SNTP" on page 98.

Example

The following command deletes the SNTP server with the IP address 148.35.16.248:

```
delete sntpserver ipaddress=148.35.16.248
```

DISABLE SNTP

Syntax

```
disable sntp
```

Parameters

None.

Description

This command disables the SNTP client software on the switch. The default setting for SNTP is disabled.

Example

The following command disables SNTP on the switch:

```
disable sntp
```

ENABLE SNTP

Syntax

```
enable sntp
```

Parameters

None.

Description

This command enables the SNTP client software on the switch. The default setting for SNTP is disabled. With SNTP enabled, the switch will obtain its date and time from an SNTP server, assuming that you have specified a server IP address with "ADD SNTPSERVER PEER|IPADDRESS" on page 90.

Example

The following command enables the SNTP client software:

```
enable sntp
```

PURGE SNTP

Syntax

```
purge sntp
```

Parameters

None.

Description

This command clears the SNTP configuration and disables the SNTP server. To disable SNTP and retain the configuration, see “DISABLE SNTP” on page 92.

Example

The following command clears the SNTP configuration and disables SNTP:

```
purge sntp
```

SET DATE

Syntax

`set date=`*`dd-mm-yyyy`*

Parameter

date	Specifies the date for the switch in day-month-year format.

Description

This command sets the date on the switch. You can use this command to set the switch's date if you are not using an SNTP server. The AT-9400 Series switch has an onboard battery that maintains the date even when the unit is powered off or reset.

Example

The following command sets the switch's date to December 11, 2004:

```
set date=11-12-2004
```

SET SNTP

Syntax

```
set sntp [dst=enabled|disabled] [pollinterval=value]
[utcoffset=value]
```

Parameters

dst	Enables or disables daylight savings time.
pollinterval	Specifies the time interval between two successive queries to the SNTP server. The range is 60 to 1200 seconds. The default is 600 seconds.
utcoffset	Specifies the time difference in hours between UTC and local time. The range is -12 to +12 hours. The default is 0 hours.

Description

This command enables or disables daylight savings time and sets the polling and UTC offset times for the SNTP client software.

Note
The switch does not set DST automatically. If the switch is in a locale that uses DST, you must remember to enable this in April when DST begins and disable it in October when DST ends. If the switch is in a locale that does not use DST, set this option to disabled all the time.

Example

The following command enables daylight savings time, sets the poll interval to 300 seconds, and sets the UTC offset to -8 hours:

```
set sntp dst=enabled pollinterval=300 utcoffset=-8
```

SET TIME

Syntax

`set time=`*`hh:mm:ss`*

Parameter

time	Specifies the hour, minute, and second for the switch's time in 24-hour format.

Description

This command sets the time on the switch. You can use this command to set the switch's time if you are not using an SNTP server. The AT-9400 Series switch has an onboard battery that maintains the time even when the unit is powered off or reset.

Example

The following command sets the switch's time to 4:34 pm and 52 seconds:

```
set time=16:34:52
```

SHOW SNTP

Syntax

```
show sntp
```

Parameters

None.

Description

This command displays the current settings for the client SNTP software on the switch. An example of the display is shown in Figure 9.

```
SNTP Configuration:
   Status ..................... Disabled
   Server ..................... 0.0.0.0
   UTC Offset ................. +0
   Daylight Savings Time (DST) ... Enabled
   Poll Interval .............. 600 seconds
   Last Delta ................. +0 seconds
```

Figure 9. SHOW SNTP Command

The information displayed by this command is described here:

- Status - The status of the SNTP client software on the switch. The status can be either enabled or disabled. If enabled, the switch seeks its date and time from an SNTP server. The default is disabled.
- SNTP - The IP address of the SNTP server.
- UTC Offset - The time difference in hours between UTC and local time. The range is -12 to +12 hours. The default is 0 hours.
- Daylight Savings Time (DST) - The status of the daylight savings time setting. The status can be enabled or disabled.
- Poll interval - The time interval between two successive queries to the SNTP server. The range is 60 to 1200 seconds. The default is 600 seconds.
- Last Delta - The last adjustment applied to the system time. It is the drift in the system clock between two successive queries to the SNTP server.

Example

The following command displays SNTP client software information:

```
show sntp
```

SHOW TIME

Syntax

```
show time
```

Parameters

None.

Description

This command shows the system's current date and time.

Example

The following command shows the system's date and time.

```
show time
```

Chapter 6

SNMPv2 and SNMPv2c Commands

This chapter contains the following commands:

- “ADD SNMP COMMUNITY” on page 102
- “CREATE SNMP COMMUNITY” on page 104
- “DELETE SNMP COMMUNITY” on page 107
- “DESTROY SNMP COMMUNITY” on page 109
- “DISABLE SNMP” on page 110
- “DISABLE SNMP AUTHENTICATETRAP” on page 111
- “DISABLE SNMP COMMUNITY” on page 112
- “ENABLE SNMP” on page 113
- “ENABLE SNMP AUTHENTICATETRAP” on page 114
- “ENABLE SNMP COMMUNITY” on page 115
- “SET SNMP COMMUNITY” on page 116
- “SHOW SNMP” on page 118

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 5, “SNMPv1 and SNMPv2c” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD SNMP COMMUNITY

Syntax

```
add snmp community="community" [traphost=ipaddress]
[manager=ipaddress]
```

Parameters

community	Specifies an existing SNMP community string on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character such as an exclamation point. Otherwise, the quotes are optional.
traphost	Specifies the IP address of a trap receiver.
manager	Specifies the IP address of a management station to have SNMP access to the switch using the community string.

Description

This command adds the IP address of a trap receiver or a management station to an existing community string.

The TRAPHOST parameter specifies a trap receiver for the SNMP community string. This is the IP address of a device to which traps generated by the switch are sent. A community string can have up to eight IP addresses of trap receivers, but only one can be added at a time with this command.

The MANAGER parameter specifies a management station to be allowed SNMP management access to the switch using the community string. This parameter applies only to community strings with a closed status. A community string can have up to eight IP addresses of management stations, but only one can be added at a time with this command.

To create a new community string, refer to “CREATE SNMP COMMUNITY” on page 104. To view the current community strings, refer to “SHOW SNMP” on page 118.

Examples

The following command permits access by a management station with the IP address 149.212.11.22 to the switch through the “private” community string:

```
add snmp community=private manager=149.212.11.22
```

The following command adds the IP address 149.212.10.11 as a trap receiver to the "public" community string:

```
add snmp community=public traphost=149.212.10.11
```

CREATE SNMP COMMUNITY

Syntax

```
create snmp community="community" [access=read|write]
[open=yes|no|on|off|true|false] [traphost=ipaddress]
[manager=ipaddress]
```

Parameters

community — Specifies a new community string. The maximum length of a community string is 15 alphanumeric characters. Spaces are allowed. The name must be enclosed in double quotes if it includes a space or other special character such as an exclamation point. Otherwise, the quotes are optional. The string is case sensitive.

access — Specifies the access level of the new community string. Options are “read” for read only access and “write” for both read and write access. The default is “read.”

open — Specifies the open or closed status of the community string. The options are:

- yes, on, true — The community string is open, meaning any management station can use the string to access the switch. These values are equivalent.
- no, off, false — The community string is closed, meaning only those management stations whose IP addresses are assigned to the string can use it to access the switch. You can assign a management IP address to the string using the MANAGER option in this command. The default setting for a community string is closed. These values are equivalent.

traphost — Specifies the IP address of a trap receiver to receive system traps.

manager — Specifies the IP address of a management station that can use the community string to access the switch. This option applies if you specify the status of the community string as closed. A community string can have up to eight IP addresses of management stations, but only one can be assigned with this option.

Description

This command creates a new SNMP community string on the switch. The switch comes with two default community strings, "public," with an access of read only, and "private," with an access level of read and write. A switch can support up to eight community strings.

The COMMUNITY parameter specifies the new community string. The string can be up to 15 alphanumeric characters. The string is case sensitive.

The ACCESS parameter defines the access level for the new community string. The access level can be either read or read and write. The READ option specifies the read access level and the WRITE option specifies the read and write access level.

The OPEN parameters controls whether the string will have an open or closed status. If you specify YES, ON or TRUE, the string will have an open status. Any management station will be able to use the string to access the switch. If you specify NO, OFF or FALSE, the string will have a closed status and only those management stations whose IP addresses are assigned to the switch will be able to use the string. This is the default.

The TRAPHOST parameter specifies the IP address of a trap receiver to receive traps from the switch. A community string can have up to eight trap receivers, but only one can be assigned when a community string is created. To add IP addresses of trap receivers to an existing community string, see "ADD SNMP COMMUNITY" on page 102.

The MANAGER parameter specifies the IP address of a management station to be permitted SNMP access to the switch through the community string. You use this parameter when you give a community string a closed status. A community string with a closed status can only be used by those management stations whose IP addresses have been assigned to the string.

A community string can have up to eight manager IP addresses, but only one can be assigned when a community string is created. To add IP addresses of management stations to an existing community string, see "ADD SNMP COMMUNITY" on page 102.

Examples

The following command creates the new community string "serv12" with read access level and an access status of open:

```
create snmp community=serv12 access=read open=yes
```

The following command creates the new community string "wind11" with read and write access level. To limit the use of the string, its access status is specified as closed and it is assigned the IP address of the management

station that will use the string:

```
create snmp community=wind11 access=write open=no
manager=149.35.24.22
```

(The OPEN=NO parameter can be omitted from the example because closed status is the default for a new community string.)

This command creates a community string called “serv12” with a closed status. The command assigns the string the IP address of a management that can use the string and also receive SNMP traps:

```
create snmp community=serv12 access=write open=no
traphost=149.35.24.22 manager=149.35.24.22
```

DELETE SNMP COMMUNITY

Syntax

```
delete snmp community="community" traphost=ipaddress
manager=ipaddress
```

Parameters

community	Specifies the SNMP community string on the switch to be modified. The community string must already exist on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character, such as an exclamation point. Otherwise, the quotes are optional.
traphost	Specifies the IP address of a trap receiver to be removed from the community string.
manager	Specifies the IP address of a management station to be removed from the community string.

Description

This command removes the IP addresses of trap receivers and management workstations from a community string.

The TRAPHOST parameter removes the IP address of a trap receiver from an SNMP community string. Once an IP address is removed, the switch will not send SNMP traps to the trap receiver represented by the address.

The MANAGER parameter removes the IP address of a management station from the community string. A management station removed from a community string with a closed status can no longer use SNMP and the community string to manage the switch. If you remove the last management station IP address from a community string with a closed status, no SNMP management station can access the switch using that community string.

Examples

The following command deletes the IP address 149.212.11.22 of a management station from the community string "private."

```
delete snmp community=private
manager=149.212.11.22
```

The following command deletes the IP address 149.212.44.45 of a trap receiver from the community string “public.”

```
delete snmp community=public traphost=149.212.44.45
```

DESTROY SNMP COMMUNITY

Syntax

```
destroy snmp community="community"
```

Parameter

community — Specifies an SNMP community string to delete from the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character, such as an exclamation point. Otherwise, the quotes are optional.

Description

This command deletes an SNMP community string from the switch. IP addresses of management stations and SNMP trap receivers assigned to the community string are deleted as well.

Example

The following command deletes the community string "wind44":

```
destroy snmp community=wind44
```

DISABLE SNMP

Syntax

```
disable snmp
```

Parameters

None.

Description

This command disables SNMP on the switch. You cannot manage the unit from an SNMP management station when SNMP is disabled. The default setting for SNMP is disabled.

Example

The following command disables SNMP on the switch:

```
disable snmp
```

DISABLE SNMP AUTHENTICATETRAP

Syntax

```
disable snmp authenticatetrap|authenticate_trap
```

Parameters

None.

Description

This command stops the switch from sending authentication failure traps to trap receivers. However, the switch will continue to send other system traps, such as alarm traps. The default setting for sending authentication failure traps is disabled.

The AUTHENTICATETRAP and AUTHENTICATE_TRAP keywords are equivalent.

To activate the authentication failure trap, refer to "ENABLE SNMP AUTHENTICATETRAP" on page 114.

Example

The following command instructs the switch not to send authentication failure traps to SNMP trap receivers:

```
disable snmp authenticatetrap
```

DISABLE SNMP COMMUNITY

Syntax

```
disable snmp community="community"
```

Parameter

community	Specifies an SNMP community string to disable on the switch. This parameter is case sensitive. The string must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.

Description

This command disables a community string on the switch, while leaving SNMP and all other community strings active. IP addresses of management stations or trap receivers assigned to the community string are also disabled. A disabled community string cannot be used by a management station to access the switch.

Example

The following command deactivates the SNMP community string “sw1200” and the IP addresses of any management stations and trap receivers assigned to the community string:

```
disable snmp community=sw1200
```

ENABLE SNMP

Syntax

```
enable snmp
```

Parameters

None.

Description

This command activates SNMP on the switch so that you can remotely manage the unit with an SNMP application program from a management station on your network. It also enables the switch to send SNMP traps to trap receivers. The default setting for SNMP on the switch is disabled.

Example

The following command activates SNMP on the switch:

```
enable snmp
```

ENABLE SNMP AUTHENTICATETRAP

Syntax

```
enable snmp authenticatetrap|authenticate_trap
```

Parameters

None.

Description

This command configures the switch to send authentication failure traps to trap receivers. The switch sends an authentication failure trap whenever a SNMP management station attempts to access the switch using an incorrect or invalid community string, or the management station's IP address has not been added to a community string that has a closed access status.

The default setting for sending authentication failure traps is disabled. Refer to "ADD SNMP COMMUNITY" on page 102 to enter the IP addresses of the SNMP trap receivers.

The AUTHENTICATETRAP and AUTHENTICATE_TRAP keywords are equivalent.

Example

The following command configures the switch to send authentication failure traps to SNMP trap receivers:

```
enable snmp authenticatetrap
```

ENABLE SNMP COMMUNITY

Syntax

```
enable snmp community="community"
```

Parameter

community	Specifies an SNMP community string. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.

Description

This command activates a community string on the switch. The default setting for a new community string is enabled. You can use this command to enable a community string that you disabled with the DISABLE SNMP COMMUNITY command.

Example

The following command enables the SNMP community string "private":

```
enable snmp community=private
```

SET SNMP COMMUNITY

Syntax

```
set snmp community="community" [access=read|write]
[open=yes|no|on|off|true|false]
```

Parameters

community — Specifies the SNMP community string whose access level or access status is to be changed. This community string must already exist on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.

access — Specifies the new access level. Options are “read” for read only access and “write” for both read and write access. If no access level is specified, the default is “read.”

open — Specifies the open or closed access status of the community string. The options are:

- yes, on, true — The community string is open, meaning that any management station can use the string to access the switch. These options are equivalent.
- no, off, false — The community string is closed, meaning that only those management stations whose IP addresses are assigned to the string can use it to access the switch. To add IP addresses of management stations to a community string, refer to “ADD SNMP COMMUNITY” on page 102. The default setting for a community string is closed. These options are equivalent.

Description

This command changes the access level and access status of an existing SNMP community string.

Examples

The following command changes the access status for the SNMP community string "sw44" to closed:

```
set snmp community=sw44 open=no
```

The following command changes the access level for the SNMP community string "serv12" to read and write with open access:

```
set snmp community=serv12 access=write open=yes
```

SHOW SNMP

Syntax

```
show snmp [community="community"]
```

Parameter

community	Specifies a community string on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional. Default community strings are “public” and “private.”

Description

This command displays the following SNMP information:

- SNMP status - The status will be enabled or disabled. If enabled, you can manage the switch with an SNMP application program from a remote management station. If disabled, you cannot remotely manage the switch using SNMP. The default for SNMP is disabled. To enable SNMP, refer “ENABLE SNMP” on page 113. To disable SNMP, refer to “DISABLE SNMP” on page 110.
- Authentication failure traps - This status will be enabled or disabled. If enabled, the switch sends out authentication failure traps to trap receivers. If disabled, the switch will not send out authentication failure traps, but will send out other system traps. The switch sends an authentication failure trap whenever a SNMP management station attempts to access the switch using an incorrect or invalid community string, or the management station’s IP address has not been added to a community string that has a closed access status. The default setting is enabled.

  To enable authentication failure traps, refer to “ENABLE SNMP AUTHENTICATETRAP” on page 114. To disable the sending of this trap, see “DISABLE SNMP AUTHENTICATETRAP” on page 111. To add IP addresses of management stations to receive the trap, refer to the “ADD SNMP COMMUNITY” on page 102.

- SNMP community strings - The switch comes with the two default community strings public, which has read access, and private, which has read and write access. To add new community strings, see “CREATE SNMP COMMUNITY” on page 104. To delete community strings, refer to “DESTROY SNMP COMMUNITY” on page 109.
- Management station IP addresses - These are the IP addresses of management stations that can access the switch through a community

string that has a closed access status. (Management station IP addresses are displayed only when you specify a specific community string using the COMMUNITY parameter in this command.) To add IP addresses of management stations to a community string, refer to "ADD SNMP COMMUNITY" on page 102.

- Trap receiver IP addresses - These are the IP addresses of management stations to receive SNMP traps from the switch. (IP addresses or trap receivers are displayed only when you specify a specific community string using the COMMUNITY parameter in this command.) To add IP addresses to a community string, refer to "ADD SNMP COMMUNITY" on page 102.
- Access Status - If a community string shows an Open Access with Yes, the string has an open access status, meaning any management stations can use the string. A string with a Open Access of No has a closed access status; only those management stations whose IP addresses have been assigned to the string can use it. To change the access status, refer to "SET SNMP COMMUNITY" on page 116.

Examples

The following command displays the SNMP status and the community strings on the switch:

```
show snmp
```

The following command displays specific information about the "private" community string. The information includes the IP addresses of management stations that can use the string and the IP addresses of SNMP trap receivers:

```
show snmp community=private
```

Chapter 7

Port Parameter Commands

This chapter contains the following commands:

- “ACTIVATE SWITCH PORT” on page 122
- “DISABLE INTERFACE LINKTRAP” on page 123
- “DISABLE SWITCH PORT” on page 124
- “DISABLE SWITCH PORT FLOW” on page 125
- “ENABLE INTERFACE LINKTRAP” on page 126
- “ENABLE SWITCH PORT” on page 127
- “ENABLE SWITCH PORT FLOW” on page 128
- “PURGE SWITCH PORT” on page 129
- “RESET SWITCH PORT” on page 130
- “SET SWITCH PORT” on page 131
- “SET SWITCH PORT FILTERING” on page 135
- “SET SWITCH PORT RATELIMITING” on page 138
- “SHOW INTERFACE” on page 141
- “SHOW SWITCH PORT” on page 143

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information, refer to Chapter 6, “Port Parameters” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ACTIVATE SWITCH PORT

Syntax

```
activate switch port=port autonegotiate
```

Parameter

port	Specifies a port. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command prompts a port that is using Auto-Negotiation to renegotiate its settings with its end node. The command can be helpful if you believe that a port and an end node have not successfully negotiated their settings.

Example

This command forces ports 1 and 4 to renegotiate their speed and duplex mode:

```
activate switch port=1,4 autonegotiate
```

DISABLE INTERFACE LINKTRAP

Syntax

```
disable interface=port linktrap
```

Parameter

port	Specifies the port on which you want to disable SNMP link traps. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command disables SNMP link traps on a port. When disabled, the switch does not send an SNMP link trap when there is a change to the status of a link on a port.

Note
In order for the switch to send SNMP traps to SNMP trap receivers, you must activate SNMP on the unit and specify one or more trap receivers.

Example

The following command disables link traps on port 21:

```
disable interface=21 linktrap
```

DISABLE SWITCH PORT

Syntax

```
disable switch port=port
```

Parameter

port	Specifies the port to disable. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command disables a port. When a port is disabled, it stops forwarding traffic. The default setting for a port is enabled.

Example

The following command disables ports 12 and 24:

```
disable switch port=12,24
```

Equivalent Command

```
set switch port=port status=disable
```

For information, see “SET SWITCH PORT” on page 131.

DISABLE SWITCH PORT FLOW

Syntax

```
disable switch port=port flow=pause
```

Parameter

port	Specifies the port where you want to deactivate flow control. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command deactivates flow control on a port. Flow control only applies to ports operating in full duplex mode.

Example

The following command deactivates flow control on port 6:

```
disable switch port=6 flow=pause
```

Equivalent Command

```
set switch port=port flowcontrol=disable
```

For information, see "SET SWITCH PORT" on page 131.

ENABLE INTERFACE LINKTRAP

Syntax

```
enable interface=port linktrap
```

Parameter

port	Specifies the port on which you want to enable SNMP link traps. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command activates SNMP link traps on the port. When enabled, the switch sends an SNMP link trap to an SNMP trap receiver whenever there is a change to the status of a link on a port.

Note
In order for the switch to send SNMP traps, you must activate SNMP on the unit and specify one or more trap receivers.

Example

The following command enables link traps on port 21:

```
enable interface=21 linktrap
```

ENABLE SWITCH PORT

Syntax

```
enable switch port=port
```

Parameter

port	Specifies the port to enable. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command enables a port. When a port is enabled, it forwards traffic. The default setting for a port is enabled.

Example

The following command enables ports 1 to 4:

```
enable switch port=1-4
```

Equivalent Command

```
set switch port=port status=enable
```

For information, see "SET SWITCH PORT" on page 131.

ENABLE SWITCH PORT FLOW

Syntax

```
enable switch port=port flow=pause
```

Parameter

port	Specifies the port where you want to activate flow control. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command activates flow control on a port. Flow control only applies to ports operating in full duplex mode. When flow control is activated, a port sends out a PAUSE packet whenever it wants the end node to stop sending packets.

Example

The following command activates flow control on port 5:

```
enable switch port=5 flow=pause
```

Equivalent Command

```
set switch port=port flowcontrol=enable
```

For information, see “SET SWITCH PORT” on page 131.

PURGE SWITCH PORT

Syntax

```
purge switch port=port
```

Parameters

port	Specifies the port to reset. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command resets all the port's settings back to the factory default values. To reset a port and retain its settings, use "RESET SWITCH PORT" on page 130.

Example

The following example resets the settings for port 10 to the factory default values:

```
purge switch port=10
```

RESET SWITCH PORT

Syntax

```
reset switch port=port
```

Parameter

port	Specifies the port to reset. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command resets a port. The reset takes less that a second to complete. You might reset a port if it is experiencing a problem establishing a link with its end node. The port retains its current operating parameter settings. To reset a port to the factory default settings, use “PURGE SWITCH PORT” on page 129.

Example

The following command resets ports 5 to 8:

```
reset switch port=5-8
```

Equivalent Command

```
set switch port=port softreset
```

For information, see “SET SWITCH PORT” on page 131.

SET SWITCH PORT

Syntax

```
set switch port=port [description="description"]
[status=enabled|disabled]
[speed=autonegotiate|10mhalf|10mfull|100mhalf|100mfull|
1000mfull]
[mdimode=mdi|mdix|auto]
[flowcontrol=disable|enable|auto]
[fctrllimit=value]
[backpressure=yes|no|on|off|true|false|enabled|
disabled]
[bplimit=value]
[holbplimit=value]
[renegotiation=auto]
[softreset]
```

Parameters

port — Specifies the port you want to configure. You can specify more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

description — A description for the port, from 1 to 15 alphanumeric characters. Spaces are allowed but do not use special characters. If the name contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

status — Specifies the operating status of the port. The options are:

- enabled — The port forwards network traffic. This is the default setting.
- disabled — The port does not forward network traffic.

speed — Sets the speed and duplex mode of the port. The options are:

- autonegotiate — The port uses Auto-Negotiation for both speed and duplex mode. This is the default setting.
- 10mhalf — 10 Mbps and half-duplex mode.

10mfull	10 Mbps and full-duplex mode.
100mhalf	100 Mbps and half-duplex mode.
100mfull	100 Mbps and full-duplex mode.
1000mfull	1000 Mbps and full-duplex mode. (Applicable only to 1000 Mbps fiber optic ports on SFP and GBIC modules.)

Note
A 10/100/1000Base-T twisted pair port operates at 1000 Mbps only when set to Auto-Negotiation.

mdimode — Sets the wiring configuration of the port. This parameter applies only to twisted pair ports, and only when a port's speed and duplex mode are set manually. If a port is autonegotiating its speed and duplex mode, the MDI/MDIX setting is established automatically and cannot be changed. The options are:

mdi	Sets the port's configuration to MDI.
mdix	Sets the port's configuration to MDI-X.

flowcontrol — Specifies the flow control on the port. Flow control applies only to ports operating in full duplex mode. When flow control is activated, a port sends out a PAUSE packet whenever it wants the end node to stop sending packets. The options are:

disabled	No flow control. This is the default setting.
enabled	Flow control is activated.

fctrllimit — Specifies the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

backpressure — Controls back pressure on the port. Back pressure applies only to ports operating in half-duplex mode. The options are:

yes, on, true, enabled	Activates back pressure on the port. These options are equivalent.

	no, off, false, disabled	Deactivates back pressure on the port. This is the default. These options are equivalent.
bplimit	Specifies the number of cells for back pressure. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.	
holbplimit	Specifies the threshold at which the switch signals a head of line blocking event on a port. The threshold is specified in cells. A cell is 128 bytes. The range is 1 to 61,440 cells; the default is 7,168.	
renegotiation	Prompts the port to renegotiate its speed and duplex mode with the end node. This parameter only works when the port is using autonegotiation. The only option is:	
	auto	Renegotiates speed and duplex mode with the end node.
softreset	Resets the port. This parameter does not change any of a port's operating parameters.	

Description

This command sets a port's operating parameters. You can set more than one parameter at a time. For an explanation of the port parameters, refer to Chapter 6, "Port Parameters" in the *AT-S63 Management Software Menus Interface User's Guide*.

Examples

The following command disables ports 1 to 6:

```
set switch port=1-6 status=disabled
```

The following command configures port 8 to operate at 10 Mbps, half duplex:

```
set switch port=8 speed=10mhalf
```

The following command sets the speed to 100 Mbps, the duplex mode to full duplex, the wiring configuration to MDI-X, and flow control to enabled for ports 2 to 6:

```
set switch port=2-6 speed=100mfull mdimode=mdix
flowcontrol=enabled
```

The following command resets port 5:

```
set switch port=5 softreset
```

Equivalent Commands

`disable switch port=`*`port`*

For information, see “DISABLE SWITCH PORT” on page 124.

`disable switch port=`*`port`* `flow=pause`

For information, see “DISABLE SWITCH PORT FLOW” on page 125.

`enable switch port=`*`port`*

For information, see “ENABLE SWITCH PORT” on page 127.

`enable switch port=`*`port`* `flow=pause`

For information, see “ENABLE SWITCH PORT FLOW” on page 128.

`reset switch port=`*`port`*

For information, see “RESET SWITCH PORT” on page 130.

SET SWITCH PORT FILTERING

Syntax

```
set switch port=port
[bcastfiltering=yes|no|on|off|true|false|enabled|
disabled]
[bcastegressfiltering=yes|no|on|off|true|false|enabled|
disabled]
[unkmcastfiltering=yes|no|on|off|true|false]
[unkmcastegressfiltering=yes|no|on|off|true|false]
[unkucastfiltering=yes|no|on|off|true|false]
[unkucastegressfiltering=yes|no|on|off|true|false]
```

Parameters

port — Specifies the port you want to configure. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

bcastfiltering — Controls the ingress broadcast frame filter. The options are:

- yes, on, true, enabled — The port discards all ingress broadcast frames. These options are equivalent.
- no, off, false, disabled — The port forwards all ingress broadcast frames. This is the default. These options are equivalent.

bcastegressfiltering — Controls the egress broadcast frame filter. The options are:

- yes, on, true, enabled — The port discards all egress broadcast frames. These options are equivalent.
- no, off, false, disabled — The port forwards all egress broadcast frames. This is the default. These options are equivalent.

unkmcastfiltering	Controls the unknown ingress multicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown ingress multicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown ingress multicast frames. This is the default. These options are equivalent.
unkmcastegressfiltering	Controls the unknown egress multicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown egress multicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown egress multicast frames. These options are equivalent.
unkucastfiltering	Controls the unknown ingress unicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown ingress unicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown ingress unicast frames. This is the default. These options are equivalent.
unkucastegressfiltering	Controls the unknown egress unicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown egress unicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown egress unicast

frames. This is the default. These options are equivalent.

Description

This command discards ingress and egress broadcast packets as well as unknown unicast and multicast packets on a port. When you activate this feature on a port, the port discards all ingress or egress packets of the type specified. The default setting for each type of packet filter is disabled.

Examples

The following command activates the ingress broadcast filter on ports 4 and 23 so that the ports discard all ingress broadcast packets:

```
set switch port=4,23 bcastfiltering=yes
```

The following command activates the unknown egress multicast and unicast filters on ports 3 and 6 so that the ports discard all unknown egress multicast and unicast packets:

```
set switch port=3,6 unkmcastegressfiltering=yes
unkucastegressfiltering=yes
```

This comand disables the unknown ingress unicast filter on port 24 so that the port again accepts all unknown ingress unicast packets:

```
set switch port=24 unkucastfiltering=no
```

SET SWITCH PORT RATELIMITING

Syntax

```
set switch port=port
[bcastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[bcastrate=value]
[mcastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[mcastrate=value]
[unkucastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[unkucastrate=value]
```

Parameters

port	Specifies the port you want to configure. You can specify more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).	
bcastratelimiting	Enables or disables rate limit for ingress broadcast packets. The options are:	
	yes, on, true, enabled	Activates broadcast packet rate limiting on the port. The options are equivalent. The rate limit is set with the BCASTRATE parameter.
	no, off, false, disabled	Deactivates broadcast packet rate limit on the port. This is the default. The options are equivalent.
bcastrate	Specifies the maximum number of ingress broadcast packets a switch port accepts each second. The range is 0 to 262,134 packets. The default is 262,134 packets	

mcastratelimiting	Enables or disables a rate limit for ingress multicast packets. The options are:	
	yes, on, true, enabled	Activates multicast packet rate limit on the port. The options are equivalent.
	no, off, false, disabled	Deactivates multicast packet rate limit on the port. This is the default. The options are equivalent.
mcastrate	Specifies the maximum number of ingress multicast packets a switch port accepts each second. The range is 0 to 262,134 packets. The default is 262,134 packets.	
unkucastratelimiting	Enables or disables rate limit for unknown ingress unicast packets. The options are:	
	yes, on, true, enabled	Activates unknown unicast packet rate limit on the port. The options are equivalent.
	no, off, false, disabled	Deactivates unknown unicast packet rate limit on the port. This is the default. The options are equivalent.
unkucastrate	Specifies the maximum number of ingress unknown unicast packets a switch port accepts each second. The range is 0 to 262,134 packets. The default is 262,134 packets.	

Description

This command sets the maximum number of ingress packets a port accepts each second. Packets exceeding the threshold are discarded. You can enable the rate limiting threshold independently for broadcast, multicast and unknown unicast packets.

Examples

The following command activates rate limiting for ingress broadcast and multicast packets on port 6. It sets a threshold of 20,000 packets per second for broadcast packets and 100,000 for multicast packets:

```
set switch port=6 bcastratelimiting=yes bcastrate=20000
mcastratelimiting=yes mcastrate=100000
```

The following command sets a threshold of 150,000 packets per second for unknown ingress unicast packets on ports 15 and 17:

```
set switch port=15,17 unkucastratelimiting=yes
unkucastrate=150000
```

The following command disables the rate limiting feature for ingress broadcast packets on port 24:

```
set switch port=24 bcastratelimiting=no
```

SHOW INTERFACE

Syntax

```
show interface[=port]
```

Parameter

port — Specifies the port whose interface information you want to display. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22). All ports are displayed if you omit the port number.

Description

This command displays the contents of the interface MIB for a specific port. An example of the information displayed by this command is shown in Figure 10.

```
ifIndex.............................. 1
ifMtu................................ 9198
ifSpeed.............................. 100000000
ifAdminStatus........................ Up
ifOperStatus......................... Up
ifLinkUpDownTrapEnable............... Enabled
```

Figure 10. SHOW INTERFACE Command

This command provides the following information about a port:

- ifIndex - The index of the interface in the interface table.
- ifMTU - The size, in octets, of the largest packet that can be transmitted on the port.
- ifSpeed - An estimate of the port's current bandwidth, in bits per second. This MIB object is zero (0) when the port does not have a link to an end node.
- ifAdminStatus - The configured state of the port, one of the following:

  Up - The port is up.

  Down - The port is down.

- ifOperStatus - The current operational status of the port, one of the following:

  Up - A valid link exists between the port and the end node.

Down - The port and the end node have not established a link.

unknown - The port status is unknown.

- ifLinkUpDownTrapEnable - Whether or not link traps have been enabled for the port, one of the following:

  Enabled - Link traps are enabled. To disable link traps, see “DISABLE INTERFACE LINKTRAP” on page 123.

  Disabled - Link traps are disabled. To enable link traps, see “ENABLE INTERFACE LINKTRAP” on page 126.

Example

The following command displays information about port 21:

```
show interface=21
```

SHOW SWITCH PORT

Syntax

```
show switch port[=port]
```

Parameter

port	Specifies the port whose parameter settings you want to view. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22). All ports are displayed if you omit the port number.

Description

This command displays a port's current operating specifications, such as speed and duplex mode. The command displays the following port information. (For an example of the information displayed by this command, see Figure 11 on page 147.)

- Port Description - Displays the name of the port. The default name is "Port_" followed by the port number. To configure a port's name, refer to "SET SWITCH PORT" on page 131.
- Port Type - Displays the IEEE standard of a port. For example, the port type for a twisted pair port on an AT-9424Ti/SP switch is 10/100/1000Base-T.
- Status - Displays whether the port is currently enabled or disabled. When disabled, a port does not forward network traffic. The default is enabled. To disable or enable a port, refer to "DISABLE SWITCH PORT" on page 124, "ENABLE SWITCH PORT" on page 127, or "SET SWITCH PORT" on page 131.
- Link State - Displays the current link state between the port and the end node. If the port has established a link with an end node, link state will be "Up." If there is no link, link state will be "Down."
- Configured Speed/Duplex - Displays the current configured settings for speed and duplex mode on the port. The setting of "Auto" indicates the port has been set to Auto-Negotiation, the default setting. To adjust a port's speed and duplex mode, refer to "SET SWITCH PORT" on page 131.
- Configured MDI Crossover - Displays the current configured setting for MDI/MDIX on the port. If the port is set to Auto-Negotiation, this field displays N/A, because the MDI/MDIX setting is set automatically on the port. A value only appears in this field if you disable Auto-Negotiation on a twisted pair port and set MDI/MDIX manually. This

field does not apply to a fiber optic port. To adjust a port's MDI/MDIX setting, refer to "SET SWITCH PORT" on page 131.

- Actual Speed/Duplex - Displays the current operating speed and duplex mode of a port. This field displays no value (—) if the port does not have a link to an end node or has been disabled.
- Actual MDI Crossover- Displays the current operating MDI/MDIX setting of a twisted pair port. This field displays no value (—) if the port does not have a link to an end node or has been disabled. This field does not apply to a fiber optic port.
- Flow Control Status and Flow Control Threshold - Displays the status of flow control on a port. Flow control applies to ports operating in full duplex mode and is used by a port to stop an end node from sending packets when its ingress buffer is full. The default setting is disabled. The threshold marks the point at which flow control is activated. The threshold is measured in cells of 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.To set flow control, refer to "DISABLE SWITCH PORT FLOW" on page 125, "ENABLE SWITCH PORT FLOW" on page 128, or "SET SWITCH PORT" on page 131.
- Backpressure Status and Backpressure Threshold - Displays the status of backpressure on a port. Backpressure applies to ports operating in half duplex mode. A port uses backpressure to stop an end node from sending packets when its ingress buffer is full. The default setting is disabled. The threshold marks the point at which backpressure is activated. The threshold is measured in cells of 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.To set backpressure, refer to "SET SWITCH PORT" on page 131.
- HOL Blocking Prevention Threshold - Displays the threshold at which the switch signals a head of line blocking event. This event occurs when switch ports are unable to forward packets to another switch port because its egress queues are full. The switch responds to this event by instructing the other switch ports to discard any packets in their ingress queues that are destined for the oversubscribed port. The threshold is measured in cells of 128 bytes. The range is 0 to 8191 cells. The default is 682.
- Broadcast Ingress Filtering - Displays the status of ingress broadcast filtering. If enabled, the port discards all ingress broadcast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 135.
- Broadcast Egress Filtering - Displays the status of egress broadcast filtering. If enabled, the port discards all egress broadcast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 135.
- Unknown Multicast Ingress Filtering - Displays the status of unknown ingress multicast filtering. If enabled, the port discards all unknown ingress multicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 135.

- Unknown Multicast Egress Filtering - Displays the status of unknown egress multicast filtering. If enabled, the port discards all unknown egress multicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 135.
- Unknown Unicast Ingress Filtering - Displays the status of unknown ingress unicast filtering. If enabled, the port discards all unknown ingress unicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 135.
- Unknown Unicast Egress Filtering - Displays the status of unknown egress unicast filtering. If enabled, the port discards all unknown egress unicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 135.
- Broadcast Rate Limiting Status and Broadcast Rate - Displays the status of the broadcast rate limiting feature. If enabled, the port limits the number of ingress broadcast packets per second to the rate specified. Ingress broadcast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to "SET SWITCH PORT RATELIMITING" on page 138.
- Multicast Rate Limiting Status and Multicast Rate - Displays the status of the multicast rate limiting feature. If enabled, the port limits the number of ingress multicast packets per second to the rate specified. Ingress multicast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to "SET SWITCH PORT RATELIMITING" on page 138.
- Unknown Unicast Rate Limiting Status and Unknown Unicast Rate - Displays the status of the unicast rate limiting feature. If enabled, the port limits the number of unknown ingress unicast packets per second to the rate specified. Unknown ingress unicast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to "SET SWITCH PORT RATELIMITING" on page 138.
- PVID - Displays the port's VLAN ID number. This number is equivalent to the VID of the VLAN where the port is currently an untagged member. The default is 1, the VID of the Default_VLAN. To add a port to an existing VLAN or to create a new VLAN, refer to "ADD VLAN" on page 516 and "CREATE VLAN" on page 518.
- Port Priority - Displays the Class of Service priority assigned to the port. This priority level applies to all ingress untagged packets received on the port. The default setting is 0. At the default setting, all ingress untagged packets received on the port are stored in the egress port's Q1 egress queue. To set this parameter, refer to "SET SWITCH PORT PRIORITY OVERRIDEPRIORITY" on page 305. To adjust the mappings of priority levels to egress queues, see "SET QOS COSP" on page 303.

- Override Priority - Displays whether the Class of Service priority level in ingress tagged packets is ignored when determining the egress queue for storing the packets. If this parameter is displaying Yes, the switch ignores the priority level in tagged packets and uses the priority level assigned to the port to determine the egress queue. The default setting is No. At the default setting the priority level in tagged packets is used to determine the appropriate egress queue. To set this parameter, refer to "SET SWITCH PORT PRIORITY OVERRIDEPRIORITY" on page 305. To adjust the mappings of priority levels to egress queues, see "SET QOS COSP" on page 303.
- Mirroring State - Displays the state of port mirroring on the switch. If port mirroring has been activated on the switch, this field will contain Enabled. If port mirroring has not been activated on the switch, the default setting, this field will contain Disabled. To configure port mirroring, refer to "SET SWITCH MIRROR" on page 194 and "SET SWITCH PORT MIRROR" on page 195.
- Is this mirror port mirror - Displays whether the port is functioning as the destination port of a port mirror. This field only appears if port mirroring has been activated on the switch. This field displays No if the port is not the destination port and Yes if it is the destination port.

For further details on port parameters, refer to Chapter 6, "Port Parameters" in the *AT-S63 Management Software Menus Interface User's Guide*.

Note
The information for an SFP or GBIC module includes additional nonadjustable operating specifications of the module.

An example of the information displayed by this command is shown in Figure 11 on page 147.

```
Port #11 Information:

Port Description ..................... Port_11
Port Type ............................ 10/100/1000Base-T
Status ............................... Enabled
Link State ........................... Up
Configured Speed/Duplex .............. Auto
Configured MDI Crossover ............. N/A
Actual Speed/Duplex .................. 100 Mbps/Full Duplex
Actual MDI Crossover ................. MDIX
Flow Control Status .................. Disabled
Flow Control Threshold ............... 7935 cells
Backpressure Status .................. Disabled
Backpressure Threshold ............... 7935 cells
HOL Blocking Prevention Threshold .... 682 cells
Broadcast Ingress Filtering .......... Disabled
Broadcast Egress Filtering ........... Disabled
Unknown Multicast Ingress Filtering .. Disabled
Unknown Multicast Egress Filtering ... Disabled
Unknown Unicast Ingress Filtering .... Disabled
Unknown Unicast Egress Filtering ..... Disabled
Broadcast Rate Limiting Status ....... Disabled
Broadcast Rate ....................... 262143 packet/second
Multicast Rate Limiting Status ....... Disabled
Multicast Rate ....................... 262143 packet/second
Unknown Unicast Rate Limiting Status . Disabled
Unknown Unicast Rate ................. 262143 packet/second
PVID ................................. 1
Port Priority (0-7) 0=Low 7=High...... 0
Override Priority .................... No
Mirroring State....................... Disabled
```

Figure 11. SHOW SWITCH PORT Command

Examples

The following command displays the operating settings for all ports:

```
show switch port
```

The following command displays the operating settings for port 14:

```
show switch port=14
```

Chapter 8

Port Statistics Commands

This chapter contains the following commands:

- “RESET SWITCH PORT COUNTER” on page 150
- “SHOW SWITCH COUNTER” on page 151
- “SHOW SWITCH PORT COUNTER” on page 154

Note
For background information on port statistics, refer to Chapter 6, “Port Parameters” in the *AT-S63 Management Software Menus Interface User’s Guide*.

RESET SWITCH PORT COUNTER

Syntax

```
reset switch port=port counter
```

Parameter

port	Specifies the port whose statistics counters you want to return to zero. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command returns a port's statistics counters to zero.

Example

The following command returns the counters on ports 14 and 15 to zero:

```
reset switch port=14-15 counter
```

SHOW SWITCH COUNTER

Syntax

```
show switch counter
```

Parameters

None.

Description

This command displays operating statistics, such as the number of packets received and transmitted, and the number of CRC errors, for the entire switch. An example of the display is shown in Figure 12.

```
Port: All

Bytes Rx ......... 983409801      Bytes Tx ......... 965734443
Frames Rx ........ 815423         Frames Tx ........ 691396
Bcast Frames Rx... 107774         Bcast Frames Tx .. 1853
Mcast Frames Rx .. 11429          Mcast Frames Tx .. 0
Frames 64 ........ 110509         Frames 65-127 .... 15192
Frames 128-255 ... 1928           Frames 256-511 ... 442
Frames 512-1023 .. 157796         Frames 1024-1518.. 1221024
CRC Error ........ 0              Jabber ........... 0
No. of Rx Errors . 0              No. of Tx Errors . 0
UnderSize Frames . 0              OverSize Frames .. 0
Fragments ........ 0              Collision ........ 0
Frames 1519-1522 . 0              Dropped Frames ... 0
```

Figure 12. SHOW SWITCH COUNTER Command

The command provides the following information:

Bytes Rx
Number of bytes received by the switch.

Bytes Tx
Number of bytes transmitted by the switch.

Frames Rx
Number of frames received by the switch.

Frames Tx
Number of frames transmitted by the switch.

Bcast Frames Rx
Number of broadcast frames received by the switch.

Bcast Frames Tx
Number of broadcast frames transmitted by the switch.

Mcast Frames Rx
Number of multicast frames received by the switch.

Mcast Frames Tx
Number of multicast frames transmitted by the switch.

Frames 64
Frames 65-127
Frames 128-255
Frames 256-511
Frames 512-1023
Frames 1024-1518
Frames 1519-1522
Number of frames transmitted from the port, grouped by size.

CRC Error
Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received by the switch.

Jabber
Number of occurrences of corrupted data or useless signals appearing on the switch.

No. of Rx Errors
Number of receive errors.

No. of Tx Errors
Number of transmit errors.

Undersize Frames
Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received by the switch.

Oversize Frames
Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received by the switch.

Fragments
Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received by the switch.

Collision
Number of collisions that have occurred on the switch.

Dropped Frames
Number of frames successfully received and buffered by the switch, but discarded and not forwarded.

Example

The following command displays the switch's operating statistics:

```
show switch counter
```

SHOW SWITCH PORT COUNTER

Syntax

```
show switch port=port counter
```

Parameter

port	Specifies the port whose statistics you want to view. You can specify more than one port at a time. To view all ports, do not specify a port.

Description

This command displays the operating statistics for a port on the switch. Examples of the statistics include the number of packets transmitted and received, and the number of CRC errors. For an example of the display and definitions of the statistics, refer to “SHOW SWITCH COUNTER” on page 151.

Examples

The following command displays the operating statistics for port 14:

```
show switch port=14 counter
```

The following command displays the operating statistics for all ports:

```
show switch port counter
```

Chapter 9

MAC Address Table Commands

This chapter contains the following commands:

- “ADD SWITCH FDB|FILTER” on page 156
- “DELETE SWITCH FDB|FILTER” on page 158
- “RESET SWITCH FDB” on page 160
- “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 161
- “SHOW SWITCH AGINGTIMER|AGEINGTIMER” on page 162
- “SHOW SWITCH FDB” on page 163

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 7, “MAC Address Table” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD SWITCH FDB|FILTER

Syntax

```
add switch fdb|filter destaddress|macaddress=macaddress
port=port vlan=name|vid
```

> **Note**
> The FDB and FILTER keywords are equivalent.

Parameters

destaddress ***or*** macaddress	Specifies the static unicast or multicast address to be added to the switch's MAC address table. The parameters are equivalent. The address can be entered in either of the following formats: xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx
port	Specifies the port(s) to which the MAC address is to be assigned. You can specify only one port if you are adding a unicast address. You can specify more than one port if you are entering a multicast address.
vlan	Specifies the name or the VID of the VLAN to which the node designated by the MAC address is a member.

Description

This command adds static unicast and multicast MAC addresses to the switch's MAC address table. A MAC address added with this command is never timed out from the MAC address table, even when the end node or, in the case of a multicast address, the multicast application is inactive.

If you are entering a static multicast address, the address must be assigned to the port when the multicast application is located and to the ports where the host nodes are connected. Assigning the address only to the port where the multicast application is located will result in the failure of the multicast packets to be properly forwarded to the host nodes.

Examples

The following command adds the static MAC address 00:A0:D2:18:1A:11 to port 7. It assumes the port where the MAC address is to be assigned is a member of the Default_VLAN:

```
add switch fdb macaddress=00A0D2181A11 port=7
vlan=default_vlan
```

The following command adds the multicast MAC address 01:00:51:00:00 10 to ports 1 to 5. The ports belong to the Engineering VLAN:

```
add switch fdb macaddress=010051000010 port=1-5
vlan=Engineering
```

DELETE SWITCH FDB|FILTER

Syntax

```
delete switch fdb|filter
macaddress|destaddress=macaddress vlan=name|vid
type|status=static|staticunicast|staticmulticast|dynamic|
dynamicunicast|dynamicmulticast
```

Note
The FDB and FILTER keywords are equivalent.

Parameters

macaddress ***or*** destaddress	Deletes a specific dynamic or static unicast or multicast MAC address from the MAC address table. The address can be entered in either of the following formats: xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx This parameter must be accompanied with the VLAN parameter.	
vlan	Specifies the VLAN containing the port(s) where the address was learned or assigned. The VLAN can be specified by name or VID. This parameter must be used with the MACADDRESS and DESTADDRESS parameters.	
type ***or*** status	Deletes specific types of MAC addresses. Options are:	
	static	Deletes all static unicast and multicast MAC addresses.
	staticunicast	Deletes all static unicast addresses.
	staticmulticast	Deletes all static multicast addresses.
	dynamic	Deletes all dynamic unicast and multicast MAC addresses.
	dynamicunicast	Deletes all dynamic unicast addresses.
	dynamicmulticast	Deletes all dynamic multicast addresses.

Description

This command deletes dynamic and static unicast and multicast addresses from the switch's MAC address table.

> **Note**
> You cannot delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

Examples

The following command deletes the static MAC address 00:A0:D2:18:1A:11 from the table. The port where the address was learned or assigned is part of the Default_VLAN, which has a VID of 1:

```
delete switch fdb macaddress=00A0D2181A11 vlan=1
```

The following command deletes the MAC address 00:A0:C1:11:22:44 from the table. The port where the address was learned or assigned is part of the Sales VLAN:

```
delete switch fdb macaddress=00a0c1112244 vlan=sales
```

The following command deletes all dynamic MAC addresses learned on the ports that belong to the Default_VLAN:

```
delete switch fdb macaddress=dynamic vlan=default_vlan
```

The following command deletes all dynamic MAC addresses:

```
delete switch fdb type=dynamic
```

The following command deletes all static unicast MAC addresses:

```
delete switch fdb type=staticunicast
```

RESET SWITCH FDB

Syntax

```
reset switch fdb [port=port]
```

Parameter

port	Specifies the port whose dynamic MAC addresses you want to delete from the MAC address table. You can specify more than one port at a time.

Description

This command deletes the dynamic MAC addresses learned by the switch. You can delete all the dynamic addresses of addresses learned on a specific port. After a port's dynamic MAC addresses have been deleted, the port begins to learn new addresses.

Example

The following command deletes all the dynamic MAC addresses in the switch's MAC address table:

```
reset switch fdb
```

The following command deletes all the dynamic MAC addresses learned in port 5:

```
reset switch fdb port=5
```

SET SWITCH AGINGTIMER|AGEINGTIMER

Syntax

```
set switch agingtimer|ageingtimer=value
```

Parameter

agingtimer ***or*** ageingtimer	Specifies the aging timer for the MAC address table. The value is in seconds. The range is 0 to 1048575. The default is 300 seconds (5 minutes). The parameters are equivalent.

Description

The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

Setting the aging timer to 0 disables the timer. No dynamic MAC addresses are aged out and the table stops learning new addresses after reaching maximum capacity.

To view the current setting for the MAC address aging timer, refer to "SHOW SWITCH AGINGTIMER|AGEINGTIMER" on page 162.

Example

The following command sets the aging timer to 120 seconds (2 minutes):

```
set switch agingtimer=120
```

SHOW SWITCH AGINGTIMER|AGEINGTIMER

Syntax

```
show switch agingtimer|ageingtimer
```

Parameters

None.

Description

This command displays the current setting for the aging timer. The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. To set the aging timer, refer to “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 161.

Figure 13 illustrates the information displayed by this command.

```
Aging interval: 300 second(s)
```

Figure 13. SHOW SWITCH AGINGTIMER|AGEINGTIMER Command

Example

The following command displays the current setting for the MAC address aging timer:

```
show switch agingtimer
```

SHOW SWITCH FDB

Syntax

```
show switch fdb [macaddress|destaddress=macaddress]
[port=port] [type|status=static|staticunicast|
staticmulticast|dynamic|dynamicunicast|dynamicmulticast]
[vlan=name]
```

Parameters

address — Specifies a MAC address. Use this parameter to determine the port on the switch on which a particular MAC address was learned (dynamic) or assigned (static). The address can be entered in either of the following formats:

xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

port — Specifies a port on the switch. Use this parameter to view all addresses learned on a particular port. You can specify more than one port.

type ***or*** status — Displays specific types of MAC addresses. Options are:

static	Displays all static unicast and multicast MAC addresses.
staticunicast	Displays all static unicast addresses.
staticmulticast	Displays all static multicast addresses.
dynamic	Displays all dynamic unicast and multicast MAC addresses.
dynamicunicast	Displays all dynamic unicast addresses.
dynamicmulticast	Displays all dynamic multicast addresses.

vlan — Specifies a VLAN name. Use this parameter to view the MAC addresses learned or assigned to the ports of a particular VLAN on the switch.

Note
You can specify more than one parameter at a time with this command.

Description

This command displays the unicast and multicast MAC addresses learned or assigned to the ports on the switch and stored in the switch's MAC address table.

Figure 14 is an example of the information displayed by this command for unicast addresses.

```
Switch Forwarding Database
Total Number of MAC Addresses: 121
VLAN ID  MAC Address          Port     Status
-------------------------------------------------------------
0        01:80:C1:00:02:01    0        Static (fixed, non-aging)
1        00:a0:d2:18:1a:c8    1        Dynamic
1        00:a0:c4:16:3b:80    2        Dynamic
1        00:a0:12:c2:10:c6    3        Dynamic
1        00:a0:c2:09:10:d8    4        Dynamic
1        00:a0:33:43:a1:87    4        Dynamic
1        00:a0:12:a7:14:68    4        Dynamic
1        00:a0:d2:22:15:10    4        Dynamic
1        00:a0:d4:18:a6:89    4        Dynamic
```

Figure 14. SHOW SWITCH FDB Command - Unicast Addresses

Note
The first address in the unicast MAC address table is the address of the switch.

The columns are defined here:

- VLAN ID - The ID number of the VLAN where the port is an untagged member.
- MAC - The dynamic or static unicast MAC address learned on or assigned to the port.
- Port - The port where the address was learned or assigned. The MAC address with port 0 is the address of the switch.
- Status - The type of address: static or dynamic.

Figure 15 is an example of a multicast address.

```
Multicast Switch Forwarding Database
Total Number of MCAST MAC Addresses: 1
MAC Address        VLANID  Type    Port Maps (U:Untagged T:Tagged)
-------------------------------------------------------------
01:00:51:00:00:01  1       Static  U:1-4
                                   T:
```

Figure 15. SHOW SWITCH FDB Command - Multicast Addresses

The columns are defined here:

- MAC Address - The static or dynamic unicast MAC address.
- VLAN ID - The ID number of the VLAN where the port is an untagged member.
- Type - The type of the address: static or dynamic.
- Port Maps - The tagged and untagged ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different groups.

Examples

The following command displays all the static and dynamic unicast MAC addresses in the switch's MAC address table:

```
show switch fdb
```

The following command displays just the static unicast MAC addresses:

```
show switch fdb type=static
```

The following command displays the static and dynamic multicast addresses:

```
show switch fdb type=multicast
```

The following command displays just the static multicast addresses:

```
show switch fdb type=staticmulticast
```

The following command displays the port where the MAC address 00:A0:D2:18:1A:11 was learned (dynamic) or added (static):

```
show switch fdb address=00A0D2181A11
```

The following command displays the MAC addresses learned on port 2:

```
show switch fdb port=2
```

The following command displays the MAC addresses learned on the ports in the Sales VLAN:

```
show switch fdb vlan=sales
```

The following command displays the static MAC addresses on port 17:

```
show switch fdb port=17 type=static
```

Chapter 10

Static Port Trunking Commands

This chapter contains the following commands:

- “ADD SWITCH TRUNK” on page 168
- “CREATE SWITCH TRUNK” on page 170
- “DELETE SWITCH TRUNK” on page 172
- “DESTROY SWITCH TRUNK” on page 173
- “SET SWITCH TRUNK” on page 174
- “SHOW SWITCH TRUNK” on page 175

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information and guidelines on static port trunking, refer to Chapter 8, “Static and LACP Port Trunks” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD SWITCH TRUNK

Syntax

```
add switch trunk=name [tgid=id_number] port=port
```

Parameters

trunk	Specifies the name of the static port trunk to be modified.
tgid	Specifies the ID number of the static port trunk to be modified. The range is 1 to 6. This parameter is optional.
port	Specifies the port to be added to the port trunk. You can add more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

Description

This command adds ports to an existing static port trunk. To initially create a static port trunk, refer to “CREATE SWITCH TRUNK” on page 170.

Caution
Disconnect all network cables from the ports of the trunk on the switch before using this command. Adding a port to a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

Note
If the port you are adding will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you check to see if its settings are appropriate prior to adding it to the trunk. If the port will not be the lowest numbered port, then its settings are changed to match the settings of the existing ports in the trunk.

Note
If the port to be added to a trunk is already a member of another static trunk, you must first remove it from its current trunk assignment. To remove ports from a trunk, see “DELETE SWITCH TRUNK” on page 172.

Example

The following command adds port 5 to a port trunk called load22:

```
add switch trunk=load22 port=5
```

CREATE SWITCH TRUNK

Syntax

```
create switch trunk=name port=ports
[select=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

Parameters

trunk	Specifies the name of the trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters are allowed.
port	Specifies the ports to be added to the port trunk. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).
select	Specifies the load distribution method. Options are:

macsrc	Source MAC address.
macdest	Destination MAC address.
macboth	Source address/destination MAC address.
ipsrc	Source IP address.
ipdest	Destination IP address.
ipboth	Source address/destination IP address.

Description

This command creates a static port trunk. To create the trunk, you specify the ports on the switch that will constitute the trunk.

Caution
Do not connect the cables to the trunk ports on the switches until after you have created the trunk in the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Note
Before creating a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port to be in the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the AT-S63 management software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

Note
All ports in a trunk must operate at the same speed. When you include port 23R or 24R in a trunk and the port transitions to redundant uplink status, the port speed is automatically adjusted to 1000 Mbps. If the other ports in the trunk are operating at a different speed, port trunking may be unpredictable. Because of these port speed variables, Allied Telesyn suggests that you not include port 23R or 24R in a port trunk.

Note
If the ports that are to constitute the new trunk are already members of another static trunk, you must first remove them from their current trunk assignment. To remove ports from a static trunk, see "DELETE SWITCH TRUNK" on page 172.

Examples

The following command creates a static port trunk using ports 3 through 6. The command names the trunk "load22" and sets the load distribution method to destination MAC address.

```
create switch trunk=load22 port=3-6 select=macdest
```

The following command creates a port trunk consisting of ports 15,17, and 22. The command names the trunk "trunk4". No load distribution method is specified, so the default source and destination MAC addresses method is used:

```
create switch trunk=trunk4 port=15,17,22
```

DELETE SWITCH TRUNK

Syntax

```
delete switch trunk=name port=port
```

Parameters

trunk	Specifies the name of the static port trunk to be modified.
port	Specifies the port to be removed from the existing port trunk. You can specify more than one port at a time.

Description

This command removes ports from a static port trunk. To completely remove a port trunk from a switch, see “DESTROY SWITCH TRUNK” on page 173.

Caution
Disconnect all data cables from the ports of the trunk on the switch before using this command. Removing a port from a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

Note
You cannot remove ports from a trunk that has only two ports because a static trunk must have a minimum of two ports.

Example

The following command removes port 9 from a port trunk called Dev_trunk:

```
delete switch trunk=Dev_trunk port=9
```

DESTROY SWITCH TRUNK

Syntax

```
destroy switch trunk=name
```

Parameter

trunk	Specifies the name of the trunk to be deleted.

Description

This command deletes a static port trunk from a switch. After a port trunk has been deleted, the ports that made up the trunk can be connected to different end nodes.

> **Caution**
> Disconnect the cables from the port trunk on the switch before destroying the trunk. Deleting a port trunk without first disconnecting the cables can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

Example

The following command deletes the trunk called load22 from the switch:

```
destroy switch trunk=load22
```

SET SWITCH TRUNK

Syntax

```
set switch trunk=name
select=macsrc|macdest|macboth|ipsrc|ipdest|ipboth
```

Parameters

trunk	Specifies the name of the static port trunk.	
select	Specifies the load distribution method. Options are:	
	macsrc	Source MAC address.
	macdest	Destination MAC address.
	macboth	Source address/destination MAC address.
	ipsrc	Source IP address.
	ipdest	Destination IP address.
	ipboth	Source address/destination IP address.

Description

This command changes the load distribution method of an existing static port trunk.

Example

The following command changes the load distribution method of a trunk named “Load11” to source MAC address:

```
set switch trunk=Load11 select=macsrc
```

SHOW SWITCH TRUNK

Syntax

```
show switch trunk
```

Parameters

None.

Description

This command displays the names, ports, and load distribution methods of the static port trunks on the switch. An example of the command is shown in Figure 16.

```
Trunk group ID ............ 2
   Trunk status ........... UP
   Trunk group name ....... Server11
   Trunk method ........... SRC/DST MAC
   Ports .................. 12-16
```

Figure 16. SHOW SWITCH TRUNK Command

The command displays the following information:

- Trunk group ID - The ID number of the static port trunk.
- Trunk status - The operational status of the trunk. If the trunk has established a link with the other device, status will be UP. If the trunk has not establish a link or the ports in the trunk are disabled, status will be DOWN.
- Trunk group name - The name of the static port trunk.
- Trunk method - One of the following load distribution methods:

SRC MAC	Source MAC address.
DST MAC	Destination MAC address.
SRC/DST MAC	Source address/destination MAC address.
SRC IP	Source IP address.
DST IP	Destination IP address.
SRC/DST IP	Source address/destination IP address.

- Ports - The ports of the static port trunk.

Example

The following command displays port trunking information:

```
show switch trunk
```

Chapter 11
LACP Port Trunking Commands

This chapter contains the following commands:

- “ADD LACP PORT” on page 178
- “CREATE LACP AGGREGATOR” on page 179
- “DELETE LACP PORT” on page 181
- “DESTROY LACP AGGREGATOR” on page 182
- “DISABLE LACP” on page 183
- “ENABLE LACP” on page 184
- “SET LACP AGGREGATOR” on page 185
- “SET LACP SYSPRIORITY” on page 187
- “SET LACP STATE” on page 188
- “SHOW LACP” on page 189

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information and guidelines on LACP port trunks, refer to Chapter 8, “Static and LACP Port Trunks” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD LACP PORT

Syntax

```
add lacp aggregator=name port=port
```

Parameters

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
port	Specifies the port to be added to the aggregator. You can add more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

Description

This command adds ports to an existing aggregator. You must identify the aggregator by its name. To display the names of the aggregators on the switch, refer to “SHOW LACP” on page 189. To create an aggregator, refer to “CREATE LACP AGGREGATOR” on page 179.

Caution
A network cable should not be connected to a port on the switch until after the port is added to the aggregator. Connecting the cable before the port is a part of an aggregator can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Note
Before adding a port to an aggregator, verify that the port’s speed is set to Auto-Negotiation or 100 Mbps, full-duplex. Aggregate trunks do not support half-duplex mode.

Examples

The following command adds ports 8 and 22 to an aggregator named “agg_1”:

```
add lacp aggregator=agg_1 port=8,22
```

CREATE LACP AGGREGATOR

Syntax

```
create lacp aggregator=name|adminkey=0xkey port=port
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

Parameters

aggregator — Specifies a name for the new aggregator. The name can be up to 20 alphanumeric characters. No spaces or special characters are allowed. If no name is specified, the default name is DEFAULT_AGG followed by a number.

adminkey — Specifies an adminkey number for the aggregator. This is a hexadecimal number in the range of 0x1 to 0xffff. If this parameter is omitted, the default adminkey of the lowest numbered port in the aggregator is used.

port — Specifies the ports of the aggregator. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

distribution — Specifies the load distribution method, which can be one of the following:

- macsrc — Source MAC address.
- macdest — Destination MAC address.
- macboth — Source and destination MAC addresses. This is the default.
- ipsrc — Source IP address.
- ipdest — Destination IP address.
- ipboth — Source and destination IP addresses.

If this parameter is omitted, the source and destination MAC addresses load distributed method is selected by default.

Description

This command creates an LACP aggregator. Note the following when creating a new aggregator:

- You can specify either a name or an adminkey but not both when creating a new aggregator.
- When you create a new aggregator by specifying a name, the adminkey is based on the operator key of the lowest numbered port in the aggregator.
- When you create an aggregator by specifying an adminkey, the aggregator's default name is DEFAULT_AGG followed by the port number of the lowest numbered port in the aggregator. For instance, an aggregator of ports 12 to 16 is given the name DEFAULT_AGG12.
- Before creating an aggregator, you should verify that the ports that will be members of the aggregator are set to Auto-Negotiation or 100 Mbps, full-duplex. Aggregate trunks do not support half-duplex mode.
- All the ports of an aggregator must be untagged ports of the same VLAN.
- You cannot change the name or adminkey of an existing aggregator. That function requires deleting the aggregator and recreating it.

Caution

Do not connect the cables to the ports of the aggregator on the switch until after you have configured LACP and the aggregators on both devices that will be interconnected by the trunk. Connecting the cables before configuring the aggregators and activating the protocol will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Examples

The following command creates an LACP aggregator named "sw_agg_1" of ports 1 through 4. The load distribution method is source MAC address. Since the aggregator is being created by name, the default operator key for port 1, the lowest numbered port in the aggregator, becomes the adminkey:

```
create lacp aggregator=sw_agg_1 port=1-4 distribution=macsrc
```

The following command creates an LACP aggregator of ports 10, 12, 15 to 18 with an adminkey number of 0x7A. The default name for the aggregator is DEFAULT_AGG10 because the command specifies an adminkey and because port 10 is the lowest numbered port in the aggregator. Since no load distribution method is specified, the source and destination MAC addresses load distributed method is used by default:

```
create lacp adminkey=0x7A port=10,12,15-18
```

DELETE LACP PORT

Syntax

```
delete lacp aggregator=name port=port
```

Parameters

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
port	Specifies the port to delete from an aggregator. You can delete more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

Description

This command removes a port from an aggregator. You must identify the aggregator by its name. To display the names of the aggregators on the switch, refer to "SHOW LACP" on page 189. To completely remove an aggregator, see "DESTROY LACP AGGREGATOR" on page 182.

Caution
Disconnect the network cable from a port before removing it from an aggregator. Removing a port without first disconnecting the cable can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Example

The following command removes port 9 from the "lacp_server" aggregator:

```
delete lacp aggregator=lacp_server port=9
```

DESTROY LACP AGGREGATOR

Syntax

```
destroy lacp aggregator=name|adminkey=0xkey
```

Parameter

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
adminkey	Specifies the adminkey number of the aggregator. This is a hexadecimal number between 0x1 and 0xffff.

Description

This command deletes an LACP aggregator from the switch. You can identify the aggregator by its name or adminkey number. To display the names and adminkeys of the aggregators on the switch, refer to “SHOW LACP” on page 189.

Caution
Disconnect the network cables from the ports of the aggregator before performing this command. Deleting the aggregator without first disconnecting the cables can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Example

The following command deletes an aggregator named “agg_15”:

```
destroy lacp aggregator=agg_15
```

The following command deletes an aggregator with an adminkey number of 0x1A:

```
destroy lacp adminkey=0x1a
```

DISABLE LACP

Syntax

```
disable lacp
```

Parameters

None.

Description

This command disables LACP on the switch. The default is disabled.

> **Caution**
> Do not disable LACP if there are defined aggregators without first disconnecting all cables connected to the aggregate trunk ports. Otherwise, a network loop may occur, resulting in a broadcast storm and poor network performance.

Example

The following command disables LACP on the switch:

```
disable lacp
```

Equivalent Command

```
set lacp state=disable
```

For information, see "SET LACP STATE" on page 188.

ENABLE LACP

Syntax

```
enable lacp
```

Parameters

None.

Description

This command activates LACP on the switch. The default is disabled.

Example

The following command activates LACP:

```
enable lacp
```

Equivalent Command

```
set lacp state=enable
```

For information, see “SET LACP STATE” on page 188.

SET LACP AGGREGATOR

Syntax

```
set lacp aggregator=name|adminkey=key
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

Parameters

aggregator	Specifies the name of the aggregator you want to modify. The name is case-sensitive.	
adminkey	Specifies the adminkey number of the aggregator you want to modify. This is a hexadecimal number between 0x1 and 0xffff.	
distribution	Specifies one of the following load distribution methods:	
	macsrc	Source MAC address.
	macdest	Destination MAC address.
	macboth	Source address/destination MAC address. This is the default.
	ipsrc	Source IP address.
	ipdest	Destination IP address.
	ipboth	Source address/destination IP address.

Description

This command modifies the load distribution method of an existing LACP aggregator. You can identify the aggregator by its name or adminkey. To display the names and adminkeys of the aggregators on the switch, refer to "SHOW LACP" on page 189.

Note
You cannot change the name or adminkey of an existing aggregator.

Examples

The following command changes the load distribution method of an LACP aggregator titled "agg_5" to the source MAC address method:

```
set lacp aggregator=agg_5 distribution=macsrc
```

The following command changes the load distribution method of an LACP aggregator with the adminkey 0x22 to the destination MAC address method:

```
set lacp adminkey=0x22 distribution=macdest
```

SET LACP SYSPRIORITY

Syntax

```
set lacp syspriority=0x priority
```

Parameters

syspriority	Specifies the LACP system priority value for a switch. This is a hexadecimal value from 0x1 to 0xffff. The lower the number, the higher the priority. The default is 0x0080.

Description

This command sets the LACP priority of the switch. LACP uses the priority to resolve conflicts between two switches to decide which switch makes the decision about which ports to aggregate.

Example

The following command sets the LACP priority on the switch to 0x8000:

```
set lacp syspriority=0x8000
```

SET LACP STATE

Syntax

```
set lacp state=enable|disable
```

Parameters

state — Specifies the state of LACP on the switch. The options are:

- enable — Enables LACP.
- disable — Disables LACP. This is the default.

Description

This command enables or disables LACP on the switch.

Caution
Do not disable LACP if there are defined aggregators without first disconnecting all cables connected to the aggregate trunk ports. Otherwise, a network loop might occur, resulting in a broadcast storm and poor network performance.

Example

The following command activates LACP on the system:

```
set lacp state=enable
```

Equivalent Commands

```
disable lacp
```

For information, see “DISABLE LACP” on page 183.

```
enable lacp
```

For information, see “ENABLE LACP” on page 184.

SHOW LACP

Syntax

```
show lacp [port=port] [aggregator] [machine=port]
```

Parameter

port	Specifies the port(s) to display. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).
aggregator	Displays information about the aggregators.
machine	Specifies the LACP machine state for a port or ports on the system.

Description

This command displays the configuration and/or machine states of the ports, and/or the aggregators. Entering the command without any parameters displays general LACP status information. Figure 17 illustrates the information displayed by this command.

```
Status  ..........................: Enable
Mac Address .......................: 00-21-46-A7-B4-43
Priority   ........................: 0x0080
Collector delay  ..................: 0 Seconds
```

Figure 17. SHOW LACP Command

The command displayed the following information:

- Status - Whether the LACP protocol is enabled or disabled on the switch.
- MAC Address - The MAC address of the switch.
- Priority - The LACP system priority value assigned to the switch.

The PORT parameter displays LACP port information. Figure 18 illustrates the information displayed by this parameter. For definitions, refer to the IEEE 802.3ad standard.

```
Port ............. 05
Aggregator ....... LACP sw22
ACTOR                                  PARTNER
=========================================
Actor Port ............. 05          Partner Port ......... 00
Selected ............... SELECTED    Partner System ....... 00-30-84-AB-EF-CD
Oper Key ............... 0xf705      Oper Key  ............ 0xff07
Oper Port Priority  .... 0x0005      Oper Port Priority ... 0x0007
Individual ............. NO          Individual ........... NO
Synchronized............ YES         Synchronized.......... YES
Collecting  ............ YES         Collecting ........... YES
Distributing ........... YES         Distributing ......... YES
Defaulted .............. NO          Defaulted ............ NO
Expired ................ NO          Expired .............. NO
Actor Churn   .......... YES         Partner Churn ........ YES
```

Figure 18. SHOW LACP Command with the PORT Parameter

The AGGREGATOR parameter displays information about each existing aggregator. Figure 19 illustrates the information displayed by this parameter.

```
Aggregator # 1 ..... DEFAULT_AGG5
Admin Key .......... 0x0001
Oper Key ........... 0x0045
Speed .............. 1000 Mbps
Distribution Mode .. MACBoth
Ports configured ... 5-8
Ports in LAGID...... 5-8
Aggregated Port .... 5-8
```

Figure 19. SHOW LACP Command with the AGGREGATOR Parameter

Examples

The following command displays general LACP status information:

```
show lacp
```

The following command displays the LACP configuration for ports 13 and 16:

```
show lacp port=13,16
```

The following command displays the configuration of the aggregators on the system:

```
show lacp aggregator
```

The following command displays the LACP machine states for each port on the system:

```
show lacp machine
```

Chapter 12

Port Mirroring Commands

This chapter contains the following commands:

- “SET SWITCH MIRROR” on page 194
- “SET SWITCH PORT MIRROR” on page 195
- “SHOW SWITCH MIRROR” on page 196

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 9, “Port Mirroring” in the *AT-S63 Management Software Menus Interface User’s Guide*.

SET SWITCH MIRROR

Syntax

```
set switch mirror=port
```

Parameter

mirror — Specifies the destination port for the port mirror. This is the port where the traffic from the source ports will be copied. You can specify only one port as the destination port. Specifying “0” (zero) disables port mirroring.

Description

This command enables mirroring and specifies the destination port, or disables mirroring. To select the source ports, refer to “SET SWITCH PORT MIRROR” on page 195.

Examples

The following command enables mirroring and makes port 11 the destination port:

```
set switch mirror=11
```

The following command disables port mirroring:

```
set switch mirror=0
```

SET SWITCH PORT MIRROR

Syntax

```
set switch port=port mirror=none|rx|tx|both
```

Parameters

port — Specifies the source port of a port mirror. You can specify more than one port. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

mirror — Specifies which traffic on the source ports is to be mirrored to the destination port. The options are:

- rx — Specifies ingress mirroring.
- tx — Specifies egress mirroring.
- both — Specifies both ingress and egress mirroring.
- none — Removes a port as a source port.

Description

This command specifies the source ports of a port mirror. If the port mirror already has source ports, the new source ports are added to the existing ports. You can also use the command to remove source ports.

You must set the destination port before you can select the source ports. To set the destination port, refer to "SET SWITCH MIRROR" on page 194.

Examples

The following command specifies ports 16 and 17 as new source ports for the port mirror. Only the ingress traffic is mirrored:

```
set switch port=16-17 mirror=rx
```

The following command removes ports 5, 7, and 10 as source ports of a port mirror:

```
set switch port=5,7,10 mirror=none
```

SHOW SWITCH MIRROR

Syntax

```
show switch mirror
```

Parameters

None.

Description

This command displays the source and destination ports of a port mirror on the switch. An example is shown in Figure 20.

```
Port Mirroring:
Mirroring State ..................... Enabled
Mirror-To (Destination) Port ........ 22
Ingress (Rx) Mirror (Source) Ports .. 1,3
Egress (Tx) Mirror (Source) Ports ... 1,3,11-13
```

Figure 20. SHOW SWITCH MIRROR Command

The command provides the following information about the port mirror:

- Mirroring State - The port mirroring status, Enabled or Disabled. If port mirroring is disabled on the switch, only this line is displayed by the command.
- Mirror-To (Destination) Port - The port functioning as the destination port.
- Ingress (Rx) Mirror (Source) Port - The port(s) whose ingress (received) traffic is mirrored.
- Egress (Tx) Mirror (Source) Port - The port(s) whose egress (transmitted) traffic is mirrored.

Example

The following command displays the status and ports of a port mirror:

```
show switch mirror
```

Chapter 13

Networking Stack

This chapter contains the following commands:

- "DELETE IP ARP" on page 198
- "DELETE TCP" on page 199
- "RESET IP ARP" on page 200
- "SET IP ARP TIMEOUT" on page 201
- "SHOW IP ARP" on page 202
- "SHOW IP ROUTE" on page 203
- "SHOW TCP" on page 204

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 10, "Networking Stack" in the *AT-S63 Management Software Menus Interface User's Guide*.

DELETE IP ARP

Syntax

```
delete ip arp [ipaddress|all]
```

Parameter

ipaddress	Specifies the IP address of an ARP entry to delete from the ARP table.
all	Specifies the deletion of all temporary ARP entries in the table.

Description

This command deletes specific or all temporary ARP entries from the ARP table.

Example

The following command deletes the ARP entry with the IP address of 192.168.1.1:

```
delete ip arp 192.168.1.1
```

DELETE TCP

Syntax

```
delete tcp indexnumber
```

Parameter

indexnumber — Specifies the internal socket ID number assigned to the connection. Enter the index number of the TCP connection you want to delete. The range is 0 to 65535 with a default of 0. To display the index numbers, refer to "SHOW TCP" on page 204.

Description

This command deletes a TCP connection. You can use the command to end a Telnet, SSH or web browser management session of a switch.

Example

The following command deletes TCP connection number 12:

```
delete tcp 12
```

RESET IP ARP

Syntax

```
reset ip arp
```

Parameter

None

Description

This command resets the ARP table by deleting all of the temporary entries in the table.

Example

The following command deletes all the temporary entries in the ARP table:

```
reset ip arp
```

SET IP ARP TIMEOUT

Syntax

```
set ip arp timeout=integer
```

Parameter

timeout — The range is 1 to 260000 seconds. The default setting is 400 seconds.

Description

This command prevents the table from becoming full with inactive entries. It allows you to set the timer for removing temporary entries in the ARP table. Inactive temporary entries in the ARP table are timed out according to the ARP cache timeout value which is set with the timeout option.

Example

The following command sets the timer to 600 seconds:

```
set ip arp timeout=600
```

SHOW IP ARP

Syntax

```
show ip arp
```

Parameter

None

Description

This command displays the IP addresses stored in the ARP table. An example is show in Figure 21.

```
Interface   IP Address     MAC Address         Type
-------------------------------------------------------------
loopback    127.0.0.1      00:00:00:00:00:00   PERMANENT
eth0        149.22.22.22   00:30:84:32:8A:5B   TEMPORARY
eth0        149.22.22.1    00:30:84:32:12:42   TEMPORARY
eth0        149.22.22.101  00:30:84:32:8A:1B   TEMPORARY
eth0        149.22.22.27   00:30:84:32:6A:11   TEMPORARY
eth0        149.22.22.86   00:30:84:32:81:22   TEMPORARY
```

Figure 21. SHOW IP ARP Command

The columns are defined here:

- Interface - The network interface of a table entry. The switch has two network interfaces. The “loopback” designation represents the interface used by the switch for internal diagnostics. The “eth0” designation represents the Ethernet network interface.
- IP Address and MAC Address - The IP addresses and their corresponding MAC addresses.
- Type - The type of ARP entry. An entry can be permanent, meaning it can never be deleted from the table, or temporary. Only the “loopback” entry is permanent. All “eth0” entries are temporary.

Example

The following command displays the ARP table.

```
show ip arp
```

SHOW IP ROUTE

Syntax

```
show ip route
```

Parameter

None

Description

This command displays the switch's IP route table. An example is shown in Figure 22.

```
Destination     Mask             Next Hop      Interface
-----------------------------------------------------------------
127.0.0.0       255.0.0.0        127.0.0.1     loopback
169.254.0.0     255.255.0.0      169.254.37.1  eth0
169.254.37.1    255.255.255.255  127.0.0.1     loopback
```

Figure 22. SHOW IP ROUTE Command

The columns are defined here:

- Destination - The IP address of a destination network, subnetwork, or end node.
- Mask - A filter used to designate the active part of the destination IP address. A binary 1 in the mask indicates an active bit in the address while a binary 0 indicates that the corresponding bit in the address is not.
- Next Hop - The IP address of the next intermediary device to reaching the destination network, subnetwork, or end node.
- Interface - The interface on the switch where the next hop is located. The switch has two interfaces. The interface "loopback" is for internal diagnostics only. The other interface is "eth0."

Example

The following command displays the IP route table:

```
show ip route
```

SHOW TCP

Syntax

```
show tcp
```

Parameter

None

Description

This command displays the TCP connections and the TCP global information which is MIB variables defined in TCP group. An example is show in Figure 23.

```
TCP MIB parameters, counters
------------------------------------
RTO min (ms):          1000   RTO max (ms):          240000
Max connections:       30
Active Opens:          0      Passive Opens:         0
Attempt Fails:         0      Established Resets:    0
Current Established:   0
In Segs:               0      In Segs Error:         0
Out Segs:              0      Out Segs Retran:       0
Out Segs with RST:     0

TCO Connections:
Total number of TCP Listening sockets: 2
Total number of TCP connections: 2
Index    Local Address      Foreign Address       State
-------------------------------------------------------------
0        0.0.0.0:80         0.0.0.0:0             LISTEN
1        0.0.0.0:23         0.0.0.0:0             LISTEN
4        169.254.37.1:23    169.254.37.138:1051   ESTABLISHED
24       169.254.37.1:80    169.254.37.101:1075   ESTABLISHED
```

Figure 23. SHOW TCP Command

The parameters in the TCP MIB Parameters, Counters section are defined here:

- RTO min (ms) and RTO max (min) - Retransmit time algorithm parameters.
- Max connections - The maximum number of TCP connections allowed.
- Active Opens - The number of active TCP opens. Active opens initiate connections.

- Passive Opens - The number of TCP passive opens. Passive opens are issued to wait for a connection from another host.
- Attempt Fails - The number of failed connection attempts.
- Established Resets - The number of connections established but have not been reset.
- Current Established - The number of current connections.
- In Segs - The number of segments received.
- In Segs Error - The number of segments received with an error.
- Out Segs - The number of segments transmitted.
- Out Segs Retran - The number of segments retransmitted.
- Out Segs with RST - The number of segments transmitted with the RST bit set.

The columns in the TCP Connections section are described here:

- Total Number of TCP Listening sockets - The number of active listening sockets. There can be a maximum of three listening sockets. One is for the Telnet server, another for SSH, and the last for the web browser server. If a server is disabled, its listening socket does not appear in the table.
- Total Number of TCP connections - The number of active Telnet, SSH, and web browser connections to the switch.
- Index - The internal socket ID number assigned to the connection.
- Local Address - The IP address of the switch, followed by the TCP port number used by the switch for the connection. The two values are divided by a colon, as illustrated in Figure 24. The port number indicates the type of TCP connection. A port number of 23 indicates a Telnet connection, 22 an SSH connection, and 80 or 443 a web browser HTTP or HTTPS connection, respectively.

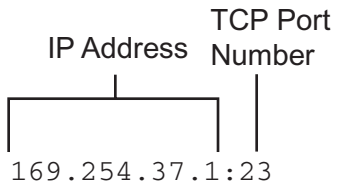

Figure 24. IP Address and TCP Port Number

- Foreign Address - The IP address of the management workstation that initiated the connection, followed by the station's TCP port number.
- State - The state of the TCP connection. A state of ESTABLISHED signals a successful TCP connection between the switch and the management workstation. For definitions of all the TCP states, refer to RFC-793.

The entries for the listening sockets for the Telnet, SSH, and web browser servers are identified in the table with a TCP state of LISTEN. If you disable a server on the switch, its corresponding LISTEN entry is removed from the table. Disabling all the servers leaves the table empty. (The SSH server is disabled by default on the switch.)

Example

The following command displays the TCP connections and the TCP global information:

```
show tcp
```

Section II

Advanced Operations

The chapters in this section contain the commands for advanced switch setup using the AT-S63 management software. The chapters include:

- Chapter 14, “File System Commands” on page 209
- Chapter 15, “File Download and Upload Commands” on page 225
- Chapter 16, “Event Log and Syslog Server Commands” on page 249
- Chapter 17, “Classifier Commands” on page 277
- Chapter 18, “Access Control List Commands” on page 289
- Chapter 19, “Class of Service (CoS) Commands” on page 299
- Chapter 20, “Quality of Service (QoS) Commands” on page 309
- Chapter 21, “Denial of Service Defense Commands” on page 353

Chapter 14

File System Commands

This chapter contains the following commands:

- “COPY” on page 210
- “CREATE CONFIG” on page 212
- “DELETE FILE” on page 213
- “FORMAT DEVICE” on page 215
- “RENAME” on page 216
- “SET CFLASH DIR” on page 218
- “SET CONFIG” on page 219
- “SHOW CFLASH” on page 221
- “SHOW CONFIG” on page 222
- “SHOW FILE” on page 223
- “SHOW FLASH” on page 224

Note
For background information on this feature, refer to Chapter 11, “File System” in the *AT-S63 Management Software Menus Interface User’s Guide*.

COPY

Syntax

`copy [cflash:]`*`sourcefile.ext`* `[cflash:]`*`destinationfile.ext`*

Parameters

sourcefile.ext	Specifies the name of the source file. If the file is stored on a compact memory flash card, precede the name with “cflash:”. If the filename contains spaces, enclose it in double quotes. Otherwise, the quotes are optional.
destinationfile.ext	Specifies the name of the destination file. To store the copy on a compact memory flash card, precede the name with “cflash:”. If the filename contains spaces, enclose in double quotes. Otherwise, the quotes are optional.

Description

This command creates a copy of an existing file. It also copies files between the switch’s file system and a compact flash memory card, for those switches that support the card.

Note the following before using this command:

- This command does not accept a directory path. When copying a file to or from a compact flash card, you must first change to the appropriate directory on the card. For instructions, refer to “SET CFLASH DIR” on page 218. The default location is the root of the flash card.
- Files with the extension UKF are encryption key pairs. These files cannot be copied, renamed, or deleted from the file system.
- The new filename must be a valid filename from 1 to 16 alphanumeric characters. The name of the copy must be unique from the other files in the file system.
- *ext* is the three-letter file extension, and can be any of the types listed in Table 4. You must give the copy the same extension as the original file.

Table 4. File Extensions and File Types

Extension	File Type
.cfg	Configuration file

Table 4. File Extensions and File Types

Extension	File Type
.cer	Certificate file
.csr	Certificate enrollment request
.key	Public encryption key
.log	Event log

Examples

The following command creates a copy of the configuration file "admin.cfg" in the switch's file system and names the copy "admin2.cfg":

```
copy admin.cfg admin2.cfg
```

The following command creates a copy of the configuration file "switch 12.cfg" in the file system and names the copy "backup.cfg":

```
copy "switch 12.cfg" backup.cfg
```

The following command copies the configuration file "9408switches.cfg" from the switch's file system to a compact flash card:

```
copy 9408switches.cfg cflash:9408switches.cfg
```

The following command copies the configuration file "sales sw12.cfg" from a compact flash card to the switch's file system and renames the file "presales_4.cfg":

```
copy cflash:"sales sw12.cfg" presales_4.cfg
```

CREATE CONFIG

Syntax

```
create config=[cflash:]filename.cfg
```

Parameter

config	Specifies the name of a new configuration file. If the filename contains spaces, enclose it in double quotes. Otherwise, the quotes are optional. To store the configuration file on a flash memory card, precede the name with “cflash:”.

Description

This command creates a new configuration file. The file contains the commands necessary to recreate the current configuration of the switch.

The CONFIG parameter specifies the name for the configuration file. The file extension must be “.cfg”. If the file already exists, it is replaced. If the file does not exist it is created.

The filename can be from 1 to 16 alphanumeric characters, not including the “.cfg” extension. Spaces are allowed. Be sure to enclose the name in double quotes if you include a space in the name. Wildcards are not allowed.

This command does not change the assignment of the active boot configuration file, which is the file the switch uses to configure itself the next time it is reset or power cycled. To change the active boot configuration file, refer to “SET CONFIG” on page 219.

Examples

The following command creates the new configuration file Switch12.cfg in the switch’s file system. The file will contain all of the commands necessary to recreate the switch’s current configuration:

```
create config=Switch12.cfg
```

The following command creates a configuration file named “l2 switches.cfg” and stores it on a compact flash card:

```
create config=cflash:”l2 switches.cfg”
```

DELETE FILE

Syntax

```
delete file=[cflash:]filename
```

Parameter

file	Specifies the name of the file to be deleted. A name with spaces must be enclosed in double quotes. Otherwise, the quotes are optional. If the file is stored on a compact memory flash card, precede the name with "cflash:".

Description

This command deletes a file from the file system or from a compact flash memory card.

Note the following before using this command:

- Deleting the configuration file that is acting as the active boot configuration file causes the switch to use its default settings the next time you reboot or power cycle the switch, unless you select another active boot configuration file. For instructions on how to change the active boot configuration file, refer to see "SET CONFIG" on page 219.
- To delete a PKI certificate, you must first remove the certificate from the certificate database using "DELETE PKI CERTIFICATE" on page 629.
- This command does not accept a directory path. To delete a file on a compact flash card, you must first change to the directory where the file is stored. For instructions, refer to "SET CFLASH DIR" on page 218.
- Files with a ".ukf" extension cannot be deleted with this command. These files are encryption key pairs. To delete an encryption key pair from the switch, refer to "DESTROY ENCO KEY" on page 618.

To list the files in the file system, refer to "SHOW FILE" on page 223.

Examples

The following command deletes the certificate enrollment request SW55a.csr:

```
delete file=SW55a.csr
```

The following command deletes the configuration file named “Switch 12.cfg” on a compact flash card:

```
delete file=cflash:"Switch 12.cfg"
```

FORMAT DEVICE

Syntax

```
format device=flash
```

Parameter

device — Specifies the device to format. The only option is "Flash" for the switch's file system.

Description

This command formats the flash memory in the switch. It deletes all files in the switch's file system, as well as all encryption keys in the key database and security certificates in the PKI certificate database. The active AT-S63 image file stored in the application block is not deleted.

Example

The following example formats the flash memory in the switch:

```
format device=flash
```

RENAME

Syntax

`rename [cflash:]`*`filename1.ext`* `[cflash:]`*`filename2.ext`*

Parameters

filename1.ext	Specifies the name of the file to be renamed. If the name contains spaces, enclose it in double quotes. Otherwise, the quotes are optional. If the file is stored on a compact memory card, precede the name with “cflash:”.
filename2.ext	Specifies the new name for the file. The filename can be from 1 to 16 alphanumeric characters, not including the filename extension. Spaces are allowed. If the name contains spaces, it must be enclosed in double quotes. The filename extension must be the same as in the original filename. The new name must be unique in the file system. If the file is stored on a compact memory card, precede the name with “cflash:”.

Description

This command renames a file in a switch’s file system or on a compact flash memory card. The source and destination file extensions must be the same.

Note the following before using this command:

- Files with the extension UKF are encryption key pairs. These files cannot be copied, renamed, or deleted from the file system.
- Renaming the active boot configuration file and then resetting the switch returns the unit to its default parameter settings, unless you save the current configuration or select another active boot configuration file. For instructions on how to change the active boot configuration file, see “SET CONFIG” on page 219.
- The command does not accept a directory path. To rename a file on a compact flash card, you must first change to the directory where the file is stored. For instructions, refer to “SET CFLASH DIR” on page 218.
- The source and destination locations must be the same.

Examples

The following command renames the file "Switch12.cfg" in the switch's file system to "Sw 44a.cfg":

```
rename Switch12.cfg "Sw 44a.cfg"
```

This command renames the file "sales_sw.cfg" on a flash memory card to "sales sw5.cfg":

```
rename cflash:sales_sw.cfg cflash:"sales sw5.cfg"
```

SET CFLASH DIR

Syntax

```
set cflash dir=directory
```

Parameter

dir Specifies the directory path.

Description

This command changes the current directory on the compact flash card.

> **Note**
> You cannot create directories on a compact flash card from the AT-S63 management software.

Example

The following command changes the current directory on a compact flash card to “configs”:

```
set cflash dir=configs
```

This command changes the current directory back to the root on the compact flash card:

```
set cflash dir=\
```

SET CONFIG

Syntax

```
set config=[cflash:]filename.cfg|none
```

Parameter

config — Specifies the name of the configuration file to act as the active configuration file for the switch. The name can be from 1 to 16 alphanumeric characters, not including the extension ".cfg". If the filename contains spaces, enclose it in double quotes.

Description

This command changes the active configuration file on a switch. The switch uses the active configuration file to configure its parameter settings when reset or power cycled. The switch also updates the active boot configuration file whenever you issue the SAVE CONFIGURATION command.

Before using this command, note the following:

- To view the name of the currently active configuration file, see "SHOW CONFIG" on page 222.
- The configuration file must already exist. To view the files, see "SHOW FILE" on page 223. Configuration files have a ".cfg" extension. To create an entirely new configuration file, refer to "CREATE CONFIG" on page 212.
- Changing the active boot configuration file does not change the current operating configuration of the switch. If you want the switch to reconfigure itself according to the configuration in the newly assigned active boot configuration file, reset or power cycle the switch.
- Entering the SAVE CONFIGURATION command after changing the active configuration file overwrites the settings in the file with the current operating settings of the switch.
- Specifying the NONE option causes the switch to operate without an active configuration file. The switch does not allow you to save any further configuration changes with the SAVE CONFIGURATION command after the NONE option is specified. If you reset the switch, it uses the BOOT.CFG configuration file to configure its settings. However, you can still use the CREATE CONFIG command to save the configuration to a new configuration file.
- You can specify a configuration file on a flash memory card for those systems that support the card. However, the switch does not copy the configuration file to its file system, but instead uses and updates the

file directly from the card. If at some point you remove the card and reset the switch, the management software will not be able to find the file and will instead use the switch's default settings.

- If the file is on a flash memory card, you must change to the directory where the file is stored before performing this command. The command does not accept a directory path. To change directories on a flash card, see "SET CFLASH DIR" on page 218. The default location is the root of the flash card.

Examples

The following command selects the file switch22.cfg as the new active boot configuration file for the switch:

```
set config=switch22.cfg
```

The following command uses the NONE option to remove the current active boot configuration file without specifying a new one. The switch does not allow you to save any further changes to the switch's configuration. If you reset the unit, it uses the BOOT.CFG file to configure its settings:

```
set config=none
```

The following command specifies the file "sw sales.cfg" on a flash memory card as the switch's active boot configuration file:

```
set config=cflash:"sw sales.cfg"
```

SHOW CFLASH

Syntax

```
show cflash
```

Parameter

None

Description

This command displays information about the compact flash card including the current directory, the number of files, how much space is used, and amount of space available. An example is shown in Figure 25.

```
Compact Flash:
-------------------------------------------------
Current Directory: \
   Number of files ............ 6
   Number of directories ...... 3
   Bytes used ................. 4468

Card Information:
   Hardware detected .......... Yes
   Serial Number .............. F000530211
   Size ....................... 124666 KB
   Used ....................       22 KB (8 files)
   Free ....................... 124644 KB
```

Figure 25. SHOW CFLASH Command

Example

```
show cflash
```

SHOW CONFIG

Syntax

```
show config [dynamic]
```

Parameter

dynamic	Displays the settings for all the switch and port parameters in command line format.

Description

This command, when used without the DYNAMIC parameter, displays two pieces of information. The first is the “Boot configuration file.” This is the configuration file the switch uses the next time it is reset or power cycled. This is also the configuration file the switch uses to save your configuration changes when you use the SAVE CONFIGURATION command. To change the boot configuration file, refer to “SET CONFIG” on page 219.

The second piece of information is the “Current Configuration.” This is the boot configuration file the switch used the last time it was reset or power cycled.

An example of the information displayed by the command is shownn in Figure 26.

```
Boot configuration file ..... "SalesSw4a.cfg" (Exists)
Current configuration ..... "SalesSw4a.cfg"
```

Figure 26. SHOW CONFIG Command

The DYNAMIC parameter displays all the switch settings in command line format for those switch parameters that have been changed from their default settings. For an example of the information displayed by the command, refer to Figure 2 on page 68.

Example

The following command displays the names of the active and current configuration files:

```
show config
```

SHOW FILE

Syntax

```
show file[=[cflash:]filename.ext]
```

Parameter

file	Specifies the name of the file to be displayed. Use double quotes to enclose the name if it contains spaces. Otherwise, the quotes are optional. To view a file on a flash memory card, precede the name with "cflash". If you do not specify a file name, the command displays a list of all files in flash memory as well as on the compact flash card.

Description

This command displays a list of the files in the switch's file system. You can use the wildcard "*" to replace any part of the filename to allow a more selective display.

You can also use this command to view the contents of a configuration file.

Examples

The following command displays all the files in the switch's file system and the current directory of the flash memory card:

```
show file
```

The following command displays all the configuration files on the switch:

```
show file=*.cfg
```

The following command displays the contents of the configuration file sw12.cfg in the switch's file system:

```
show file=sw12.cfg
```

The following command displays the contents of the configuration file boot.cfg on a compact flash card:

```
show file=cflash:boot.cfg
```

SHOW FLASH

Syntax

```
show flash
```

Parameter

None

Description

This command displays information about the file system in the switch. The information includes the number of files stored in the file system, how much space is used, and the amount of space available. An example of the information displayed by this command is shown in Figure 27.

```
Flash:
------------------------------------------------------------
  Files ..............   12288 bytes (5 files)
  Free  .............. 8211456 bytes
  Total .............. 8223744 bytes
------------------------------------------------------------
```

Figure 27. SHOW FLASH Command

Example

```
show flash
```

Chapter 15

File Download and Upload Commands

This chapter contains the following commands:

- “LOAD METHOD=LOCAL” on page 226
- “LOAD METHOD=TFTP” on page 228
- “LOAD METHOD=XMODEM” on page 232
- “UPLOAD METHOD=LOCAL” on page 236
- “UPLOAD METHOD=REMOTESWITCH” on page 238
- “UPLOAD METHOD=TFTP” on page 243
- “UPLOAD METHOD=XMODEM” on page 246

Note
For background information on this feature, refer to Chapter 12, “File Downloads and Uploads” in the *AT-S63 Management Software Menus Interface User’s Guide*..

LOAD METHOD=LOCAL

Syntax

```
load method=local destfile=appblock srcfile|file=filename
```

Parameters

method	Specifies a local download.
destfile	Specifies the application block (APPBLOCK) of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file.
srcfile *or* file	Specifies the filename of the AT-S63 image file in the file system that you want to download into the application block. If the filename contains a space, enclose it in double quotes. These parameters are equivalent.

Description

This command downloads an AT-S63 image file already stored in the switch's file system into the application block, which is the section of flash memory reserved for the active AT-S63 running image. This function makes the AT-S63 file the new active image file on the switch. This command assumes that at some earlier point you downloaded a new version of the AT-S63 image file into the file system of a switch and you now want to make that image file the switch's active image file.

When performing a local download, note the following:

- The AT-S63 manage image that you want to be the new running image for the switch must already be stored in the switch's file system.
- The command must include the DESTFILE parameter with the APPBLOCK option.
- Use the SRCFILE or FILE parameter to specify the name of the AT-S63 image file as it is stored in the switch's file system.
- The current configuration of a switch is retained when a new AT-S63 software image copied to the application block.
- After you have downloaded an image file from the file system to the application block, you can delete the image file from the file system to free up space for other files.

Caution

After downloading an AT-S63 image file into the application block from its file system, the switch resets and initializes its management software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

Example

This command downloads an AT-S63 image file already stored in the switch's file system into the application block, which is the area of flash memory reserved for the active running image. This makes the file the active image file on the switch. The name of the image file in the file system in this example is "ats63v1 2 0.img":

```
load method=local destfile=appblock srcfile="ats63v1 2
0.img"
```

A confirmation prompt is displayed. Type **Y** for yes to transfer the file to the application block or **N** for no to cancel the procedure.

LOAD METHOD=TFTP

Syntax

```
load method=tftp destfile=[cflash:]filename|appblock
server=ipaddress srcfile|file=filename
```

Parameters

method	Specifies a TFTP download.
destfile	Specifies the destination filename for the file. This is the name given to the file when it is stored in the switch's file system. The name can be from 1 to 15 alphanumeric characters, not including the three-letter extension. If the name includes spaces, enclose it in double quotes. The name must be unique from any files already stored in the file system. The command will not overwrite a preexisting file with the same name. To download a file onto a flash memory card in a switch rather than the file system, precede the name with "cflash:". The APPBLOCK option specifies the application block of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file. The APPBLOCK option is used to download a new AT-S63 image file from a TFTP server to the application block of the switch so that it functions as the new active image file on the switch.
server	Specifies the IP address of the TFTP server on the network.
srcfile ***or*** file	Specifies the filename of the file on the TFTP server to download onto the switch. If the filename contains a space, enclose the name in double quotes. These parameters are equivalent.

Description

A TFTP download uses the TFTP client software on the switch to download files onto the unit from a TFTP server on your network. For example, you might use the command to update a switch's AT-S63 image file, or to download a different boot configuration file or a SSL public key certificate. You can also use this command to download a file from a TFTP server to a flash memory card in a switch.

Note
In earlier versions of the AT-S63 management software this command also performed switch to switch file transfers for copying files from a master switch to other switches in an enhanced stack. That function is now part of "UPLOAD METHOD=REMOTESWITCH" on page 238

The DESTFILE parameter specifies a name for the file as it will be stored in the file system or a flash memory card in the switch. Enclose the name in double quotes if it contains a space. When specifying the new name of a downloaded file, be sure to give it the correct three-letter extension that corresponds to its file type. The extensions are shown in Table 5.

Table 5. File Name Extensions - Downloading Files

Extension	File Type
.cfg	AT-S63 configuration file
.cer	CA certificate
.img	AT-S63 management software image (An AT-S63 image file is assigned a named only if you are downloading the file into the switch's file system instead of the application block.)

To store a file in a flash memory card, the destination filename must be preceded with "cflash:".

The APPBLOCK option of the DESTFILE parameter refers to the switch's application block, which is the portion of flash memory reserved for the active AT-S63 image. The application block is separate from the file system. The APPBLOCK option downloads a new version of the AT-S63 image file into the application block, making it the active image file on the switch.

Note
The APPBLOCK option should only be used when downloading a new AT-S63 image file, and not with any other file type.

The equivalent FILE and SCRFILE parameters specify the name of the file on the TFTP server to download onto the switch.

Before downloading a file onto a switch using TFTP, note the following:

- A TFTP download is supported from a local, Telnet or SSH management session.

- There must be a node on your network that contains TFTP server software and the file to be downloaded must be stored on the server.
- You should start the TFTP server software before you perform the download command.
- The switch where you are downloading the file must have an IP address and subnet mask, such as a master switch. For switches without an IP address, such as a slave switch, you can perform an Xmodem download from a local management session or, alternatively, a switch to switch upload using “UPLOAD METHOD=REMOTESWITCH” on page 238.
- If you are downloading a configuration file, the switch does not automatically designate it as its active boot configuration file. To designate a configuration file as the active boot file after you have downloaded it onto the switch, refer to “SET CONFIG” on page 219.
- The AT-S63 software image can be downloaded only onto an AT-9400 Series switch.
- The current configuration of a switch is retained when a new AT-S63 software image is installed.
- The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- If you download a new AT-S63 image file and enter a filename for the DESTFILE parameter instead of APPBLOCK, the file is stored in the switch’s file system. To copy the image file from the file system to the application block so that its used by the switch as its active image file, refer to “UPLOAD METHOD=LOCAL” on page 236.

  Note
  Downloading an AT-S63 image file into a switch’s file system rather than into the application block should be perform with care. The file will take up 2 megabytes of space in the file system.

- If you download a file onto a flash memory card in the switch and later want to copy the file from the card to a switch’s file system, refer to “COPY” on page 210.

Examples

The following command downloads a new configuration file into the switch’s file system using TFTP. The configuration file is stored as “sw 111.cfg” on the TFTP server and is given the name “sw56a.cfg” when stored in the switch’s file system. The TFTP server has the IP address 149.55.55.55:

```
load method=tftp destfile=sw56a.cfg server=149.55.55.55
srcfile=”sw 111.cfg”
```

The following command downloads an SSL certificate to the switch's file system. The name of the file on the TFTP server is "sw12_ssl.cer". The same name is used for the file in the switch's file system:

```
load method=tftp destfile=sw12_ssl.cer server=149.44.44.44
srcfile=sw12_ssl.cer
```

The following command downloads a new version of the AT-S63 software image directly to the switch's application block, making it the active image file on the switch. The IP address of the TFTP server is 149.11.11.11 and the name of the image file on the server is "ats63v120.img":

```
load method=tftp destfile=appblock server=149.11.11.11
srcfile=ats63v120.img
```

Caution

After downloading an AT-S63 image file and writing it to the application block portion of flash memory, the switch resets and initializes its management software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

The following command downloads a new version of the AT-S63 image file from a TFTP server to the switch's file system, changing the name from "ats63v1_2_0.img" to "ats63.img":

```
load method=tftp destfile=ats63.img server=149.11.11.11
srcfile=ats63v1_2_0.img
```

Since the file is downloaded to the switch's file system and not to the application block, it is not used as the switch's active image file. If, at some point in the future, you want to make it the active image file, refer to "UPLOAD METHOD=LOCAL" on page 236.

This command downloads a configuration file called "sw12.cfg onto a flash memory card in the switch. The configuration file retains the same name when stored on the card. The TFTP server has the IP address 149.142.44.44:

```
load method=tftp destfile=cflash:sw12.cfg
server=149.142.44.44 srcfile=sw12.cfg
```

This command downloads an AT-S63 image file from a TFTP server to a flash memory card in the switch:

```
load method=tftp destfile=cflash:ats63.img
server=149.11.11.11 srcfile=ats63.img
```

LOAD METHOD=XMODEM

Syntax

```
load method=xmodem destfile=[cflash:]filename|appblock
```

Parameters

method — Specifies an Xmodem download.

destfile — Specifies the destination filename for the file. This is the name given to the file when it is stored in the switch's file system. The name can be from 1 to 15 alphanumeric characters, not including the three-letter extension. If the name includes spaces, enclose it in double quotes. The name must be unique from any files already stored in the file system. The command will not overwrite a preexisting file with the same name.

To download a file onto a flash memory card in a switch rather than the file system, precede the name with "cflash:".

The APPBLOCK option specifies the application block of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file. The APPBLOCK option is used to download a new AT-S63 image file into the application block so that it functions as the new active image file on the switch.

Description

An XMODEM download uses the XMODEM utility to download files onto a switch from a terminal or computer with a terminal emulator program connected to the switch's RS232 Terminal Port. You might use the command to update a switch's AT-S63 image file, or to download a different boot configuration file or a SSL public key certificate.

Note
In previous versions of the AT-S63 management software this command also performed switch to switch file transfers for copying files from a master switch to other switches in an enhanced stack. That function is now part of "UPLOAD METHOD=REMOTESWITCH" on page 238

The DESTFILE parameter specifies a name for the file. This is the name the file will be stored as in the file system on the switch. Enclose the name in double quotes if it contains a space. When specifying the new name of a

downloaded file, you must be sure to give it the correct three-letter extension, depending on the file type. The extensions are shown in Table 5 on page 229.

To download the file onto a flash memory card in the switch, precede the name with "cflash:".

The APPBLOCK option of the DESTFILE parameter refers to the switch's application block, which is the portion of flash memory reserved for the active AT-S63 image. This option downloads a new version of the AT-S63 image file into the application block, making it the active image file on the switch.

Note
The APPBLOCK option should only be used when downloading a new AT-S63 image file, and not with any other file type.

Before downloading a file onto a switch using Xmodem, note the following:

- An Xmodem download is possible only from a local management session on a switch.
- Xmodem can download a file only onto the switch where you started the local management session. It cannot download a file through enhanced stacking.
- The file to download must be stored on the computer or terminal connected to the RS232 Terminal Port on the switch.
- The transfer protocol can be Xmodem or 1K Xmodem.
- When downloading a new configuration file, the switch does not automatically designate the file as its active boot configuration file. To designate a configuration file as the active boot file, refer to "SET CONFIG" on page 219.
- The AT-S63 software image is supported only on AT-9400 Series switches.
- The current configuration of a switch is retained when a new AT-S63 software image is installed.
- The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- If you download a new AT-S63 image file and enter a filename for the DESTFILE parameter instead of APPBLOCK, the file is stored in the switch's file system. To copy an image file from the file system to the switch's application block, refer to "LOAD METHOD=LOCAL" on page 226.

Note
Downloading an AT-S63 image file into a switch's file system rather than into the application block should be perform with care. The file will take up 2 megabytes of space in the file system.

- If you download a file onto a flash memory card in the switch and later want to copy the file from the card to a switch's file system, refer to "COPY" on page 210.

Examples

The following command downloads a new configuration file onto the switch. The configuration file is given the name "switch12.cfg" in the switch's file system:

```
load method=xmodem destfile=switch12.cfg
```

The source file is not specified when downloading a file using Xmodem. Rather, after you enter the command, the management software displays a confirmation prompt followed by another prompt instructing you to begin the file transfer. To start the transfer, you use your terminal emulation program to specify the file on your workstation that you want to download.

The following command uses Xmodem to download an SSL certificate into the switch's file system and assigns it the name sw12 ssl.cer:

```
load method=xmodem destfile="sw12 ssl.cer"
```

The following command uses the APPBLOCK option of the DESTFILE parameter to download a new version of the AT-S63 software image directly to the application block, making the file the active image file on the switch:

```
load method=xmodem destfile=appblock
```

Caution
After downloading an AT-S63 image file and writing it to the application block portion of flash memory, the switch resets itself and initializes the software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

The following command downloads a configuration file onto a flash memory card in the switch. The configuration file is given the name "product_sw.cfg" on the card:

```
load method=xmodem destfile=cflash:product_sw.cfg
```

The following command downloads a new version of the AT-S63 image file to the switch's file system instead of the application block. It does this by replacing the APPBLOCK option with a filename, in this case "ats63v1_2_0.img". The image file is stored in the switch's file system with this name:

```
load method=xmodem destfile=ats63v1_2_0.img
```

Since the file is stored in the switch's file system and not the application block, the switch does not use it as its active image file. If, at some point in the future, you want to make it the active image file, use "LOAD METHOD=LOCAL" on page 226.

UPLOAD METHOD=LOCAL

Syntax

```
upload method=local destfile=[cflash:]filename
srcfile|file=appblock
```

Parameters

method	Specifies a local upload.
destfile	Specifies a filename for the AT-S63 image file. If the name contains spaces, enclose the name in quotes. To upload the active image file to a flash memory card in the switch, precede the name with “cflash:”.
srcfile *or* file	Specifies the application block (APPBLOCK), where the active AT-S63 image file is stored.

Description

This command copies the switch’s active AT-S63 image file from the application block, where the active AT-S63 image is stored, into the switch’s file system or to a flash memory card.

Note
It is unlikely you will ever need to perform this type of upload.

Note
An AT-S63 image file is approximately 2 megabytes in size. The file system in an AT-9400 Series switch is 8 megabytes in size.

The DESTFILE parameter specifies a name for the file. This is the name given to the AT-S63 image file when it is stored in the file system or on a compact flash memory card. The name should include the suffix “.img”.

The equivalent SRCFILE and FILE parameters specify APPBLOCK, for application block.

Example

The following command uploads the active AT-S63 image from the switch’s application block to the file system and assigns it the name “sw12 s63 image.img”:

```
upload method=local destfile=”sw12 s63 image.img”
srcfile=appblock
```

This command uploads the active AT-S63 image from the switch's application block to a flash memory card in the switch and assigns the file the name "s63.img":

```
upload method=local destfile=cflash:s63.img"
srcfile=appblock
```

UPLOAD METHOD=REMOTESWITCH

Syntax

```
upload method=remoteswitch
srcfile|file=filename|appblock|switchcfg
switchlist=switches [verbose=yes|no|on|off|true|false]
```

Parameters

method — Specifies a switch to switch upload.

srcfile *or* file — Specifies the file to be uploaded from the master switch. Options are:

- *filename* — Specifies the name of a configuration file in the master switch's file system.
- appblock — Uploads the master switch's active AT-S63 image file.
- switchcfg — Uploads the master switch's active boot configuration file.

switchlist — Specifies the switches in an enhanced stack to which to upload a file or the AT-S63 image file from the master switch. (To view the switches in an enhanced stack, see "SHOW REMOTELIST" on page 86.) You can specify more than one switch at a time (for example, 1,3,4).

verbose — Specifies whether to display details of the upload operation. The options are:

- yes, on, true — Display the upload details. The options are equivalent.
- no, off, false — Do not display the upload details. The options are equivalent.

Description

This command uploads a boot configuration file or an active AT-S63 file image from a master switch to other switches in an enhanced stack. This is refer to as a switch to switch upload.

This command offers a simply means for updating multiple switches in a stack. For instance, to update switches with a new version of the AT-S63 image file, you can update the master switch first and then use a switch to switch upload to update the other switches in the stack.

You can also have a master switch distribute a configuration file to the other switches. This is useful in situations where the switches will share a similar configuration because it can save you from having to configure the switches individually.

The equivalent SRCFILE and FILE parameters specify the name of the file that you want to upload from the switch. You have three options:

- *filename* - Uploads a configuration file from the master switch's file system. This differs from the SWITCHCFG parameter in that the latter uploads just the active boot configuration file, while this parameter allows you to upload any configuration file in the master switch's file system.
- APPBLOCK - Uploads the master switch's active AT-S63 image file.
- SWITCHCFG - Uploads the master switch's active boot configuration file.

The SWITCHLIST parameter specifies the switches in the enhanced stack where you want to download the management image file or configuration file. You display the switch numbers using "SHOW REMOTELIST" on page 86.

The optional VERBOSE parameter is used to monitor the progress of the upload process.

When performing a switch to switch upload, note the following:

- The command must be performed from a management session of a master switch.
- You can perform a switch to switch upload from a local, Telnet, or SSH management session.
- The master switch must have an IP address for this procedure. The address can be assigned manually or through DHCP or BOOTP. Since a master switch of an enhanced stack typically has an IP address, this should not be an issue.
- You must perform the SHOW REMOTELIST command before performing this command. The command displays the switch numbers and also allows the management software to determine which switches are in the enhanced stack. For instructions, refer to "SHOW REMOTELIST" on page 86.
- You can upload the master switch's active AT-S63 image file, its active configuration file, or another configuration file stored in its file system to other switches. You cannot upload any other type of file, such as an encryption key or SSL certificate.
- You do not specify a destination filename in a switch to switch upload. A configuration file retains its original name on the switches where it is uploaded.

- When uploading the master switch's active AT-S63 image file to another switch, the file is copied directly to the application block on the other switch, automatically making it the active image file. It is not copied to the file system. This results in a switch reset of the unit that receives the image file. Some network traffic may be lost while the switch reloads its operating software.
- After the upload of a configuration file is complete, the switch that received the configuration file marks it as the its active boot configuration file and automatically resets. Some network traffic may be lost while the switch reloads its operating software. After the reset is complete, the switch operates with the parameter settings contained in the uploaded configuration file.
- When uploading a configuration file, the command syntax gives you the choice of downloading the master switch's current boot configuration file or another configuration file in the switch's file system. To select the switch's current configuration file, use the SWITCHCFG option of the SRCFILE or FILE parameter. To upload another configuration file, omit the SWITCHCFG option and instead specify the file's name.
- If you use the SWITCHCFG option to upload the switch's current boot configuration file, the following information in the file is not included in the transfer: IP address, subnet mask, gateway address, switch name, contact, location, and the master mode setting. However, the switch receiving the configuration file does not retain its current settings to these parameters. Rather, they are returned to their default values.
- If you choose to upload a configuration file from the master switch's file system by specifying its filename, the entire file without modification is uploaded. This type of configuration file upload should be performed with care. If you upload a configuration file that contains a manually assigned IP address onto more than one switch, the switches will have the same IP address.
- A configuration file should only be uploaded onto a switch of the same model from which the configuration file originated (for example, AT-9408LC/SP to AT-9408LC/SP). Allied Telesyn does not recommend uploading a configuration file onto a switch of a different model (for example, AT-9408LC/SP to AT-9424T/SP). Undesirable switch behavior may result.
- Unlike some of the other LOAD and UPLOAD commands that support copying files to and from a compact flash memory card, this command does not. The configuration file most be stored in the master switch's file system and not on a compact flash memory card.

Examples

The following command uploads the active AT-S63 image file on a master switch to switch 2 in an enhanced stack. (Switch numbers are displayed with "SHOW REMOTELIST" on page 86.)

```
upload method=remoteswitch srcfile=appblock switchlist=2
```

The active AT-S63 image file on the master switch is indicated with the APPBLOCK option of the SRCFILE parameter.

Caution

After a switch receives the AT-S63 image file, it resets itself and initializes the software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

You can upload the AT-S63 image file from the master switch to more than one switch at a time. The following command uploads the active image file to switches 4, 8, and 15:

```
upload method=remoteswitch srcfile=appblock
switchlist=4,8,15
```

The following command uploads the switch active boot configuration file from the master switch to switches 11 and 12:

```
upload method=remoteswitch srcfile=switchcfg
switchlist=11,12
```

Since the current configuration file was designated with the SWITCHCFG option rather than its filename, the following information in the file is not included in the upload: IP address, subnet mask, gateway address, switch name, contact, location, and the master mode setting. However, the switch receiving the configuration file does not retain its current settings to these parameters. Rather, they are returned to their default values.

Caution

After a switch receives the configuration file, it resets itself and initializes the software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

The following command uploads the configuration file "sales_switches.cfg" from a master switch to switch 4:

```
upload method=remoteswitch srcfile=sales_switches.cfg
switchlist=4
```

After the switch receives the file, it marks the file as its active boot configuration file and automatically resets itself so that it starts running with the new settings.

Since the configuration file was designated by its filename, the entire file without modifications is uploaded. This type of configuration file upload should be performed with care. If the configuration file contains a command that assigns the switch a set IP address, more than one switch could end up with the same IP address.

UPLOAD METHOD=TFTP

Syntax

```
upload method=tftp destfile=[cflash:]filename
server=ipaddress srcfile|file=switchcfg|filename|appblock
```

Parameters

method	Specifies a TFTP upload.	
destfile	Specifies a filename for the uploaded file. This is the name given the file when it is stored on the TFTP server. If the name contains spaces, enclose it in quotes.	
server	Specifies the IP address of the network node containing the TFTP server software.	
srcfile *or* file	Specifies the file to be uploaded. Options are:	
	switchcfg	Uploads the switch's active boot configuration file.
	filename	Uploads a file from the switch's file system. If the file is stored on a compact flash card, precede the name with "cflash:".
	appblock	Uploads the switch's active AT-S63 image file.

Description

A TFTP upload uses the TFTP client software on the switch to upload files from the file system on the system to a TFTP server on the network. You can use the command to upload a switch's active boot configuration file or any other file from the file system, such as an SSL certificate enrollment request or a public encryption key. This command can also upload a file from a compact flash memory card in the switch to a TFTP server. You can also use the command to upload the switch's active AT-S63 software image from the application block to a TFTP server, though it is unlikely you would ever have need for that function.

When performing a TFTP upload, note the following:

- A TFTP upload is supported from a local, Telnet, or SSH management session.
- There must be a node on your network that contains the TFTP server software. The uploaded file will be stored on the server.

- Start the TFTP server software before you perform the command.
- The switch from where you are uploading the file must have an IP address and subnet mask, such as a master switch of an enhanced stack. To upload a file from a switch that does not have an IP address, such as a slave switch, you can perform an Xmodem upload from a local management session.

The DESTFILE parameter specifies a name for the file. This is the name that the file will be stored as on the TFTP server. When you name an uploaded file, you should give it the three-letter extension that corresponds to its file type. The extensions are listed in Table 6.

Table 6. File Name Extensions - Uploaded Files

Extension	File Type
.cfg	AT-S63 configuration file
.csr	CA certificate enrollment request
.log	Event log
.key	Public encryption key
.img	AT-S63 management software image

The SERVER parameter specifies the IP address of the network node containing the TFTP server software where the uploaded file will be stored.

The equivalent SRCFILE and FILE parameters specify the name of the file to be uploaded from the switch. You have three options:

- SWITCHCFG - Uploads the switch's active boot configuration file to the TFTP server.
- *filename* - Uploads a file from the switch's file system to the TFTP server. This differs from the SWITCHCFG parameter in that the latter uploads just the active boot configuration file, while this parameter can upload any file in the file system. If the file to be uploaded is stored on a compact flash memory card in the switch, precede the name with "cflash:".
- APPBLOCK - Uploads the switch's active AT-S63 image file to the TFTP server.

Examples

The following command uses TFTP to upload a configuration file called "sw22 boot.cfg" from the switch's file system to a TFTP server with an IP address of 149.88.88.88. The command stores the file on the server with

the same name that it has on the switch:

```
upload method=tftp destfile="sw22 boot.cfg"
server=149.88.88.88 srcfile="sw22 boot.cfg"
```

The following command uses TFTP to upload the switch's active configuration file from the file system to a TFTP server with the IP address 149.11.11.11. The active boot file is signified with the SWITCHCFG option rather than by its filename. This option is useful in situations where you do not know the name of the active boot configuration file. The file is stored as "master112.cfg" on the TFTP server:

```
upload method=tftp destfile=master112.cfg
server=149.11.11.11 srcfile=switchcfg
```

The following command uploads a SSL certificate enrollment request form titled "sw12_ssl_enroll.csr" from the file system to the TFTP server. It changes the name of the file to "slave5b enroll.csr":

```
upload method=tftp destfile="slave5b enroll.csr"
server=149.11.11.11 srcfile=sw12_ssl_enroll.csr
```

The following command uploads a configuration file called "sales2.cfg" from a compact flash memory card in the switch to a TFTP server with an IP address of 149.124.88.88. The command stores the file on the server with the same name that it has on the card:

```
upload method=tftp destfile=sales2.cfg server=149.124.88.88
srcfile=cflash:sales2.cfg
```

The following command uploads the switch's active AT-S63 image file to a TFTP server with an IP addresses 149.55.55.55. The file is given the name "ats63 sw12.img":

```
upload method=tftp destfile="ats63 sw12.img"
server=149.55.55.55 srcfile=appblock
```

Note
It is unlikely you will ever have cause to upload an active image file from a switch to a TFTP server. If you are considering the upload so as to update the image file on another switch, you can simplify the process by instead performing a switch to switch upload using "UPLOAD METHOD=REMOTESWITCH" on page 238.

UPLOAD METHOD=XMODEM

Syntax

```
upload method=xmodem
srcfile|file=switchcfg|filename|appblock
```

Parameters

method	Specifies an Xmodem upload.	
srcfile *or* file	Specifies the file to be uploaded. Options are:	
	switchcfg	Uploads the switch's active boot configuration file.
	filename	Specifies the name of the file in the switch's file system. If the file is stored on a compact flash card, precede the name with "cflash:".
	appblock	Uploads the switch's active AT-S63 image file.

Description

An XMODEM upload uses the Xmodem utility to upload a file from the switch's file system to a terminal or computer with a terminal emulator program connected to the serial terminal port on the switch. You can use the command to upload a switch's active boot configuration file or any other file from the file system, such as an SSL certificate enrollment request or a public encryption key. You can also use this command to upload a file on a compact flash memory card to your workstation. The command also allows you to upload the switch's active AT-S63 software image from the application block to a your terminal or workstation, though it is unlikely you would ever have need for that function.

When performing an Xmodem upload, note the following:

- An Xmodem upload must be performed from a local management session.
- Xmodem can only upload a file from the switch where you started the local management session. Xmodem cannot upload a file from a switch accessed through enhanced stacking.

The equivalent SRCFILE and FILE parameters specify the name of the file that you want to upload from the switch. You have three options:

- SWITCHCFG - Uploads the switch's active boot configuration file.
- *filename* - Uploads a file from the switch's file system. This differs from the SWITCHCFG parameter in that the latter uploads just the active boot configuration file, while this parameter can upload any file in the switch's file system. If the file to upload is on a flash memory card in the switch, precede the filename with "cflash:".
- APPBLOCK - Uploads the switch's active AT-S63 image file.

Examples

The following command uses Xmodem to upload a configuration file called "sw22 boot.cfg" from the switch's file system to the workstation where you are running the local management session:

```
upload method=xmodem srcfile="sw22 boot.cfg"
```

An Xmodem upload command does not include a destination filename. After entering the command, use your terminal emulator program to indicate where you want to store the file on your workstation and its filename.

The following command uses Xmodem to upload the switch's active configuration file from the file system to your workstation. The active boot file is signified with the SWITCHCFG option rather than by its filename. This option is useful in situations where you do not know the name of the active boot configuration file:

```
upload method=xmodem srcfile=switchcfg
```

The following command uploads a SSL certificate enrollment request named "sw12_ssl_enroll.csr" from the switch's file system to the workstation:

```
upload method=xmodem srcfile=sw12_ssl_enroll.csr
```

The following command uses Xmodem to upload a configuration file called "pre10.cfg" from a flash memory card to the workstation where you are running the local management session:

```
upload method=xmodem srcfile=cflash:pre10.cfg
```

The following command uploads the switch's active AT-S63 image file to the workstation:

```
upload method=xmodem srcfile=appblock
```

Note
It is unlikely you will ever have cause to upload an active image file from a switch to your workstation. If you are considering the upload so as to update the image file on another switch, you can simplify the process by instead performing a switch to switch upload using “UPLOAD METHOD=REMOTESWITCH” on page 238.

Chapter 16

Event Log and Syslog Server Commands

This chapter contains the following commands:

- “ADD LOG OUTPUT” on page 250
- “CREATE LOG OUTPUT” on page 252
- “DESTROY LOG OUTPUT” on page 256
- “DISABLE LOG” on page 257
- “DISABLE LOG OUTPUT” on page 258
- “ENABLE LOG” on page 259
- “ENABLE LOG OUTPUT” on page 260
- “PURGE LOG” on page 261
- “SAVE LOG” on page 262
- “SET LOG FULLACTION” on page 264
- “SET LOG OUTPUT” on page 265
- “SHOW LOG” on page 268
- “SHOW LOG OUTPUT” on page 273
- “SHOW LOG STATUS” on page 275

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on these features, refer to Chapter 13, “Event Logs and Syslog Servers” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD LOG OUTPUT

Syntax

```
add log output=output-id module=[all|module]
severity=[all|severity]
```

Parameters

output — Specifies the output definition ID number.

module — Specifies what AT-S63 events to filter. The available options are:

- all — Sends events for all modules. This is the default.
- module — Sends events for specific module(s). You can select more than one module at a time, for example, MAC,PACCESS. For a list of modules, see Table 9, “AT-S63 Modules” on page 269.

severity — Specifies the severity of events to be sent. The options are:

- all — Sends events of all severity levels.
- severity — Sends events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 271. The default is I, E, and W.

Description

This command configures an output definition.

Note
This version of the AT-S63 management software supports only syslog servers as output definitions.

There are two steps to creating a output definition from the command line interface. The first is to create the definition using “CREATE LOG OUTPUT” on page 252. With that command you assign the definition an ID number, the IP address of the syslog server, and other information.

The second step is to customize the definition by specifying which event messages generated by the switch are to be sent. This is accomplished with this command. You can customize the definition so that the switch sends all of its event messages or limit it to just a selection of events from particular modules in the AT-S63 management software. An alternative method to configuring a definition is with "SET LOG OUTPUT" on page 265.

Note
The default configuration for a new output definition is no event messages. The switch does not send any events until you customize the definition with this command or "SET LOG OUTPUT" on page 265.

The OUTPUT parameter specifies the ID number of the output definition you want to configure. The range is 2 to 20. The definition must already exist on the switch. To view the existing definitions and their ID numbers, refer to "SHOW LOG OUTPUT" on page 273.

The MODULE parameter specifies the modules whose events you want the switch to send. The AT-S63 management software consists of a number of modules. Each module is responsible for a different part of switch operation and generates its own events. The MODULE parameter's ALL option sends the events from all the modules. You can also specify individual modules, which are listed in Table 9 on page 269.

The SEVERITY parameter specifies the severity of the events to be sent. For example, you might configure the switch to send only error events of all the modules. Or, you might configure a definition so that the switch sends only warning events from a couple of the modules, such as the spanning tree protocol and the MAC address table. For a list of severity levels, refer to Table 10 on page 271.

Examples

The following command configures output definition 5 to send event messages from all modules and all severity levels:

```
add log output=3 module=all severity=all
```

The following command configures output definition 3 to send only messages related to enhanced stacking and the MAC address table with an error severity level:

```
add log output=3 module=estack,mac severity=e
```

CREATE LOG OUTPUT

Syntax

```
create log output=output-id destination=syslog
server=ipaddress
[facility=default|local1|local2|local3|local4|local5|local6
|local7] [syslogformat=extended|normal]
```

Parameters

output — Specifies an ID number that identifies the output definition. The possible output IDs are:

- 0 — Reserved for permanent (nonvolatile) storage. You cannot change or delete this ID.
- 1 — Reserved for temporary (dynamic) storage. You cannot change or delete this ID.
- 2 - 20 — Available to be used for other outputs.

destination — Specifies the destination for the log messages. The only option currently supported is:

- syslog — Forwards log messages in syslog format to a syslog server.

server — Specifies the IP address of the syslog server.

facility — Specifies a facility level to be added to the events.

- default — Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S63 management software and its modules are shown in Table 7 on page 254. This is the default setting.
- local1 to local7 — Adds a set facility code of 17 (LOCAL1) to 23 (LOCAL7) to all event messages. For a list of the levels and their corresponding codes, refer to Table 8 on page 254.

syslogformat	Specifies the format of the generated messages. The possible options are:
	extended — Messages include the date, time, and system name. This is the default.
	normal — Messages do not include the date, time, and system name.

Description

This command creates a new output definition. The switch uses the definition to send event messages to a device on your network. You can create up to nineteen output definitions.

Note
This version of the AT-S63 management software supports only syslog servers as output definitions.

After creating a output definition with this command, you must customize it by defining which event messages you want the switch to send. You can customize a definition so that the switch sends all of its event messages or limit it to just a selection of events from particular modules in the AT-S63 management software. Customizing a definition is accomplished with "ADD LOG OUTPUT" on page 250 or "SET LOG OUTPUT" on page 265.

Note
The default configuration for a new output definition is no event messages. The switch does not send events until you customize the definition.

The OUTPUT parameter specifies the ID number for the new output definition. The range is 2 to 20. Every definition must have a unique ID number.

The SERVER parameter specifies the IP address of the syslog server.

The FACILITY parameter adds a numerical code to the entries as they are sent to the syslog server. You can use this code to group entries on the syslog server according to the management module or switch that produced them. This is of particular value when a syslog server is collecting events from several difference network devices. You can specify only one facility level for a syslog server definition.

There are two approaches to using this parameter. The first is to use the DEFAULT option. At this setting, the code is based on the functional groupings defined in the RFC 3164 standard. The codes that are applicable to the AT-S63 management software and its modules are shown in Table 7.

Table 7. Default Syslog Facilities

Facility Number	Syslog Protocol Definition	Mapped Event Log Modules and Events
4	Security/ authorization messages	Security and authorization messages from the following modules: DOS, ENCO, PACCESS (802.1x), PKI, PSEC (port security), RADIUS, SSH, SSL, TACACS+, and system events such as user login and logout.
9	Clock daemon	Time-based activities and events from the following modules: TIME, SNTP, and RTC.
16	Local use 0	All other modules and events.
22	Local use 6	Physical interface and data link events from the following modules: PCFG (port configuration), PMIRR (port mirroring), PTRUNK (port trunking), STP, and VLANs.
23	Local use 7	System events related to major exceptions.

For example, the setting of DEFAULT assigns port mirroring events a code of 22 and encryption key events a code of 4.

Another option is to assign all events from a switch the same numerical code using the LOCAL1 to LOCAL2 options. Each option represents a predefined RFC 3164 numerical code. The code mappings are listed in Table 8.

Table 8. Numerical Code and Facility Level Mappings

Numerical Code	Facility Level Setting
17	LOCAL1
18	LOCAL2
19	LOCAL3
20	LOCAL4
21	LOCAL5
22	LOCAL6

Table 8. Numerical Code and Facility Level Mappings (Continued)

Numerical Code	Facility Level Setting
23	LOCAL7

For example, selecting LOCAL2 as the facility level assigns the numerical code of 18 to all events sent to the syslog server by the switch.

The SYSLOGFORMAT parameter defines the content of the events.

Examples

The following command creates output definition number 10, sends the messages to a syslog server in normal format with a facility level setting of LOCAL6:

```
create log output=10 destination=syslog server=149.65.10.99
facility=local6 syslog format=normal
```

The following command creates output definition number 18 and sends all of the messages to the syslog server. Because the FORMAT option is omitted from the command, the messages are sent in extended format, which is the default:

```
create log output=18 destination=syslog server=149.65.10.101
```

DESTROY LOG OUTPUT

Syntax

```
destroy log output=output-id
```

Parameters

output	Specifies the output definition ID number.

Description

This command deletes the specified output definition. To disable the output definition without deleting it, see “DISABLE LOG OUTPUT” on page 258.

Example

The following command destroys output definition number 3:

```
destroy log output=3
```

DISABLE LOG

Syntax

```
disable log
```

Parameters

None.

Description

This command disables the event log module. When the log module is disabled, the AT-S63 management software stops storing events in the event logs and sending events to output definitions. The default setting for the event logs is enabled.

> **Note**
> The event log module, even when disabled, still logs all AT-S63 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S63 initialization are recorded only if the event log module is enabled.

Examples

The following command disables the event log on the switch:

```
disable log
```

DISABLE LOG OUTPUT

Syntax

```
disable log output[=output-id]
```

Parameters

output	Specifies the output definition ID number to disable. Not specifying an output definition disables all definitions.

Description

This command disables an output definition. When disabled, no event messages are sent to the specified device, although the definition still exists. To permanently remove an output definition, see “DESTROY LOG OUTPUT” on page 256. To enable the output definition again, see “ENABLE LOG OUTPUT” on page 260.

Example

The following command disables (but does not delete) output definition number 7:

```
disable log output=7
```

The following command disables all configured definitions:

```
disable log output
```

ENABLE LOG

Syntax

```
enable log
```

Parameters

None.

Description

This command activates the event logs. After the log is activated, the switch immediately starts to store events in the event logs and send events to defined outputs. The default setting for the event log is enabled.

Example

The following command activates the event log module on the switch:

```
enable log
```

ENABLE LOG OUTPUT

Syntax

```
enable log output[=output-id]
```

Parameters

output	Specifies the output definition ID number to enable. The range is 2 to 20.

Description

This command enables an output definition that was disabled using “DISABLE LOG OUTPUT” on page 258.

Example

The following command enables output definition number 4:

```
enable log output=4
```

The following command enables all output definitions:

```
enable log output
```

PURGE LOG

Syntax

```
purge log[=permanent|temporary]
```

Parameter

log — Specifies the type of memory on the switch where the log file you want to purge is located. The options are:

- permanent — Permanent (nonvolatile) memory. Deletes all events stored in nonvolatile memory, which can contain up to 2,000 events.
- temporary — Temporary memory. Deletes all events stored in temporary memory, which can contain up to 4,000 events. This is the default if you do not specify the "permanent" option.

Description

This command deletes all the entries stored in an event log.

Example

The following command deletes all the entries in the event log stored in temporary memory:

```
purge log=temporary
```

The following command deletes all the entries in both event logs:

```
purge log
```

SAVE LOG

Syntax

```
save log[=permanent|temporary] filename=filename.log [full]
[module=module] [reverse] [severity=all|severity]
[overwrite]
```

Parameters

log — Specifies the source of the events you want to save to the log file. The options are:

- permanent — Permanent (nonvolatile) memory. Saves events stored in nonvolatile memory, which can contain up to 2,000 events.
- temporary — Temporary memory. Saves events stored in temporary memory, which can contain up to 4,000 events. This is the default.

filename — Specifies the filename for the log. The name can be up to 16 alphanumeric characters, followed by the extension ".log." Spaces are allowed. The filename must be enclosed in quotes if it contains spaces. Otherwise, the quotes are optional.

full — Specifies the amount of information saved to the log. Without this option, the log saves only the time, module, severity, and description for each entry. With it, the log also saves the filename, line number, and event ID.

module — Specifies the AT-S63 module whose events are to be saved. For a list of modules, refer to Table 9 on page 269. Omitting this parameter saves the events from all the modules.

reverse — Specifies the order of the events in the log. Without this option, the events are saved oldest to newest. With this option, the events are saved newest to oldest.

severity — Specifies the severity of events to be saved. The options are:

- all — Saves events of all severity levels.

severity	Saves events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, "Event Log Severity Levels" on page 271. The default is E, W, I.
overwrite	Overwrites the file if it already exists. Without this option, the command displays an error if a file with the same name already exists in the switch's file system.

Description

This command saves the current entries in an event log to a file in the file system. The parameters in the command allow you to specify which events you want saved in the log file.

Examples

The following command saves the event messages stored in the permanent event log to a file called "switch2.log". Because the MODULE and SEVERITY parameters are not included in the command, the defaults are used, which is events from all modules with an informational, error, or warning severity level:

```
save log=permanent filename=switch2.log
```

The following command saves the error messages of the VLAN module stored in the temporary event log in a file called "sw14.log.":

```
save log=temporary filename=sw14.log module=vlan severity=e
```

The following command saves informational messages from all modules in a file called "sw56.log" and overwrites the file of the same name if it already exists in the file system:

```
save log=permanent filename=sw56.log severity=i overwrite
```

SET LOG FULLACTION

Syntax

```
set log fullaction [temporary=halt|wrap]
[permanent=halt|wrap]
```

Parameters

fullaction	Specifies what happens when the logs reach maximum capacity. You can set the action separately for events stored in temporary or permanent memory. The possible actions are:	
	halt	The logs stop storing new events.
	wrap	The logs delete the oldest entries as new ones are added. This is the default.

Description

This command defines what the event logs do after they have stored the maximum number of entries. The HALT option instructs the logs to stop storing new entries. If an event log has already reached its maximum capacity, it immediately stops entering new entries. The WRAP option instructs the logs to delete the oldest entries as new entries are added.

Example

The following command configures the event log in permanent memory to stop storing new entries after it has stored the maximum number of allowed entries:

```
set log fullaction permanent=halt
```

SET LOG OUTPUT

Syntax

```
set log output=output-id [destination=syslog]
server=ipaddress
[facility=default|local1|local2|local3|local4|local5|local6
|local7] [syslogformat=extended|normal] [module=all|module]
[severity=all|severity-list]
```

Parameters

output — Specifies an ID number that identifies the output definition to be modified. The possible output IDs are:

- 0 — Reserved for permanent (nonvolatile) storage. You cannot change or delete this ID.
- 1 — Reserved for temporary (dynamic) storage. You cannot change or delete this ID.
- 2 - 20 — Available to be used for other outputs.

destination — Specifies the destination for the log messages. The only option currently supported is:

- syslog — Forwards log messages in syslog format to a syslog server.

server — Specifies a new IP address for the syslog server.

facility — Specifies a facility level to be added to the events.

- default — Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S63 management software and its modules are shown in Table 7 on page 254. This is the default setting.
- local1 to local7 — Adds a set facility code of 17 (LOCAL1) to 23 (LOCAL7) to all event messages. For a list of the levels and their corresponding codes, refer to Table 8 on page 254.

syslogformat	Specifies the format of the generated messages. The possible options are:
extended	Messages include the date, time, and system name. This is the default.
normal	Messages do not include the date, time, and system name.
module	Specifies what AT-S63 events to filter. The available options are:
all	Sends events for all modules. This is the default.
module	Sends events for specific module(s). You can select more than one module at a time, for example, MAC,PACCESS. For a list of modules, see Table 9, “AT-S63 Modules” on page 269.
severity	Specifies the severity of events to be sent. The options are:
all	Sends events of all severity levels.
severity	Sends events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 271. The defaults are I, E, and W.

Description

This command modifies an existing output definition. For further information on the FACILITY and SYSLOGFORMAT parameters, see “CREATE LOG OUTPUT” on page 252. For further information about the MODULE and SEVERITY parameters, see “ADD LOG OUTPUT” on page 250.

Note
This version of the AT-S63 management software supports only syslog servers as output definitions.

Examples

The following command changes the IP address for output definition number 5 to 149.55.55.55:

```
set log output=5 server=149.55.55.55
```

The following command modifies output definition number 6 to only send messages from the RADIUS module of all severity levels:

```
set log output=6 module=radius severity=all
```

The following command changes the facility level and message format for output definition 4. The facility level is changed to LOCAL1 (numerical code 17) and the format to normal so that the messages include only severity, module, and description:

```
set log output=11 facility=local1 syslogformat=normal
```

The following command changes syslog server definition 11 to send only spanning tree and IGMP snooping events with a severity level of error or warning:

```
set log output=11 module=stp,igmpsnooping severity=e,w
```

SHOW LOG

Syntax

```
show log=[permanent|temporary] [full] [module=module]
[reverse] [severity=severity]
```

Parameters

log — Specifies which of the two event logs you want to view. The options are:

- permanent — Displays the events stored in permanent memory.
- temporary — Displays the events stored in temporary memory. This is the default.

full — Specifies the amount of information displayed by the log. Without this option, the log displays the time, module, severity, and description for each entry. With it, the log also displays the filename, line number, and event ID.

module — Specifies the AT-S63 module whose events you want displayed. For a list of modules, refer to Table 9 on page 269.

reverse — Specifies the order of the events in the log. Without this option, the events are displayed oldest to newest. With this option, the events are displayed newest to oldest.

severity — Specifies the severity of events to be displayed. The options are:

- all — Displays events of all severity levels.
- severity — Displays events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 271. The defaults are I, E, and W.

Description

This command displays the entries stored in an event log.

An event log can display entries in two modes: normal and full. In the normal mode, a log displays the time, module, severity, and description for each entry. In the full mode, a log also displays the filename, line number, and event ID. If you want to view the entries in the full mode, use the FULL parameter. To view entries in the normal mode, omit the parameter.

The MODULE parameter displays entries generated by a particular AT-S63 module. You can specify more than one module at a time. If you omit this parameter, the log displays the entries for all the modules. Table 9 lists the modules and their abbreviations.

Table 9. AT-S63 Modules

Module Name	Description
ALL	All modules
ACL	Port access control list
CFG	Switch configuration
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands
DOS	Denial of service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	System IP configuration, DHCP, and BOOTP
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management access control list
MLD	MLD snooping
PACCESS	802.1x port-based access control

Table 9. AT-S63 Modules (Continued)

Module Name	Description
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	Port security (MAC address-based)
PTRUNK	Port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RPS	Redundant power supply
RRP	RRP snooping
RTC	Real time clock
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; Manager and Operator log in and log off events.
TACACS	TACACS+ authentication protocol
Telnet	Telnet
TFTP	TFTP
Time	System time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes
WATCHDOG	Watchdog timer

The log can display its entries in chronological order (oldest to newest), or reverse chronological order. The default is chronological order. To reverse the order, use the REVERSE parameter.

The SEVERITY parameter displays entries of a particular severity. Table 10 defines the different severity levels. You can specify more than one severity level at a time. The default is to display error, warning, and informational messages.

Table 10. Event Log Severity Levels

Value	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue may require manager attention.
I	Informational	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

An example of the event log is shown in Figure 28. The example uses the full display mode.

```
S  Date      Time      EventID    Source File:Line Number
                       Event
-----------------------------------------------------------------
I  2/01/04   09:11:02  073001     garpmain.c:259
                       garp: GARP initialized
I  2/01/04   09:55:15  083001     portconfig.c:961
                       pcfg: PortConfig initialized
I  2/01/04   10:22:11  063001     vlanapp.c:444
                       vlan: VLAN initialization succeeded
I  2/01/04   12:24:12  093001     mirrorapp.c:158
                       pmirr: Mirror initialization succeeded
I  2/01/04   12:47:08  043016     macapp.c:1431
                       mac: Delete Dynamic MAC by Port[2] succeeded
```

Figure 28. Event Log Example

The columns in the log are described below:

- S (Severity) - The event's severity. Refer to Table 10 on page 271.
- Date/Time - The date and time the event occurred.
- Event - The module within the AT-S63 software that generated the event followed by a brief description of the event. For a list of the AT-S63 modules, see Table 9 on page 269.
- Event ID - A unique number that identifies the event. (Displayed only in the full display mode.)
- Filename and Line Number - The subpart of the AT-S63 module and the line number that generated the event. (Displayed only in the full display mode.)

Examples

The following command displays all the entries in the event log stored in permanent memory:

```
show log=permanent
```

The following command displays the events stored in temporary memory in the full display mode, which adds more information:

```
show log=temporary full
```

The following command displays only those entries stored in temporary memory and associated with the AT-S63 modules FILE and QOS:

```
show log=permanent module=file,qos
```

The following command displays the error and warning entries for the AT-S63 module VLAN. Because the log is not specified, the temporary log is displayed by default:

```
show log module=vlan severity=e,w
```

SHOW LOG OUTPUT

Syntax

```
show log output[=output-id] [full]
```

Parameters

output	Specifies the output definition ID number. If an output ID number is not specified, all output definitions currently configured on the switch are displayed.
full	Displays the details of the output definition. If not specified, only a summary is displayed.

Description

This command displays output definition details. An example of the information displayed by this command is shown in Figure 29.

```
OutputID   Type           Status       Details
-------------------------------------------------------
0          Permanent      Enabled      Wrap on Full
1          Temporary      Enabled      Wrap on Full
2          Syslog         Enabled      169.55.55.55
3          Syslog         Enabled      149.88.88.88
```

Figure 29. SHOW LOG OUTPUT Command

The columns in the display are described below:

- Output ID - The ID number of the output definition. The permanent event log has the ID 0 and the temporary log has the ID 1. Syslog server definitions start with ID 2.
- Type - The type of output definition. Permanent is the permanent event log and Temporary is the temporary event log. Syslog indicates a syslog server definition.
- Status - The status of the output definition, which can be enabled or disabled.
- Details - The event log full action or a syslog server's IP address. For an event log, this column contains the log's full action. Wrap on Full indicates that the log adds new entries by deleting old entries when it reaches maximum capacity. Halt on Full means the log stops adding entries after reaching maximum capacity. To configure the full action for an event log, refer to "SET LOG FULLACTION" on page 264. For a syslog definition, this column contains the IP address of the syslog server.

An example of the information displayed by this command with the FULL parameter is shown in Figure 30.

```
Output ID ..................... 2
Output Type ................... Syslog
Status ........................ Enabled
Server IP Address ............. 149.88.88.88
Message Format ................ Extended
Facility Level ................ DEFAULT
Event Severity ................ E,W,I
Event Module .................. All
```

Figure 30. SHOW LOG OUTPUT Command with the FULL Parameter

For definitions of the parameters, refer to “SET LOG OUTPUT” on page 265.

Examples

The following command lists all the output definitions:

```
show log output
```

The following command displays the details of output definition number 5:

```
show log output=5 full
```

SHOW LOG STATUS

Syntax

```
show log status
```

Parameter

None.

Description

This command displays information about the event log feature. Figure 31 is an example of the information displayed by this command.

```
Event Log Configuration:
Event Logging ..................... Enabled
Number of Output Definitions ..... 4
```

Figure 31. SHOW LOG STATUS Command

The Event Logging field indicates whether the feature is enabled or disabled. If enabled, the switch stores events in the event logs and sends events to defined outputs. If disabled, no events are stored in the event logs or sent to defined outputs. To enable and disable the event logs, refer to "ENABLE LOG" on page 259 and "DISABLE LOG" on page 257.

The Number of Output Definitions is the sum of the two event logs plus any output definitions that you might have created. For instance, the number 4 for Number of Output Definitions in the above example indicates the existence of two output definitions in addition to the two event logs. To create new output definitions, refer to "CREATE LOG OUTPUT" on page 252 and "ADD LOG OUTPUT" on page 250.

Example

The following command displays event log status information:

```
show log status
```

Chapter 17

Classifier Commands

This chapter contains the following commands:

- “CREATE CLASSIFIER” on page 278
- “DESTROY CLASSIFIER” on page 282
- “PURGE CLASSIFIER” on page 283
- “SET CLASSIFIER” on page 284
- “SHOW CLASSIFIER” on page 287

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
For background information on this feature, refer to Chapter 14, “Classifiers” in the *AT-S63 Management Software Menus Interface User’s Guide*.

CREATE CLASSIFIER

Syntax

```
create classifier=idnumber [description="string"]
[macdaddr=macaddress|any] [macsaddr=macaddress|any]
[ethformat=ethii-untagged|ethii-tagged|802.2-
untagged|802.2-tagged|any]
[priority=integer|any] [vlan=name|1..4094|any]
[protocol=ip|arp|rarp|number|any] [iptos=integer|any]
[ipdscp=integer] [ipprotocol=protocol|number|any]
[ipdaddr=ipaddress/mask|any]
[ipsaddr=ipaddress/mask|any] [tcpsport=integer|any]
[tcpdport=integer|any] [udpsport=integer|any]
[udpdport=integer|any]
[tcpflags=[urg|ack|psh|rst|syn|fin|any]
```

Parameters

classifier	Specifies the ID number of the classifier. The number can be from 1 to 9999. Each classifier must be assigned a unique ID number. This parameter is required.
description	Specifies a description of the classifier. A description can be up to fifteen alphanumeric characters. Spaces are allowed. If it contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.
macdaddr	Specifies a destination MAC address. The address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx
macsaddr	Specifies a source MAC address. The address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx
ethformat	Specifies the type of Ethernet frame that needs to be classified. The options are: ethII-untagged ethII-tagged 802.2-untagged 802.2-tagged
priority	Specifies the user priority level in a tagged Ethernet frame. The value can be 0 to 7.

vlan	Specifies a tagged or port-based VLAN by its name or VID number.
protocol	Specifies a Layer 2 protocol. Options are: IP ARP RARP You can specify other Layer 2 protocols by entering the protocol number in either decimal or hexadecimal format. If you use the latter, precede the number with "0x".
iptos	Specifies a Type of Service value. The range is 0 to 7.
ipdscp	Specifies a DSCP value. The range is 0 to 63.
ipprotocol	Specifies a Layer 3 protocol. Options are: TCP UDP ICMP IGMP You can specify other Layer 3 protocols by entering the protocol number in either decimal or hexadecimal format. If you use the latter, precede the number with "0x".
ipdaddr	Specifies a destination IP address. The address can be of a specific node or a subnet. To filter using the IP address of a subnet, you must include a mask. A mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the Class C subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits that represent the network section of the address. The address and mask are separated by a slash (/); for example, "IPDADDR=149.11.11.0/24". No mask is necessary for the IP address of a specific end node.
ipsaddr	Specifies a source IP address. The address can be of a specific node or a subnet. If the latter, a mask must be included to indicate the subnet portion of the address. For an explanation of the mask, refer to the IPDADDR parameter.
tcpsport	Specifies a source TCP port.
tcpdport	Specifies a destination TCP port.
udpsport	Specifies a source UDP port.

udpdport Specifies a destination UDP port.

tcpflags Specifies a TCP flag. Options are

URG - Urgent
ACK - Acknowledgement
RST - Reset
PSH - Push
SYN - Synchronization
FIN - Finish

Description

This command creates a classifier. A classifier defines a traffic flow. A traffic flow consists of packets that share one or more characteristics. A traffic flow can range from being very broad to very specific. An example of the former might be all IP traffic while an example of the latter could be packets with specific source and destination MAC addresses.

You use classifiers with access control lists (ACL) and Quality of Service policies to define the traffic flow to be affected by the ACL or QoS.

If you create a classifier without any parameters, then all incoming packets are classified.

The ANY option of a parameter is used when you want to delete the current setting of a parameter without setting a new value. This leaves the parameter blank so that it applies to all packets.

Note
For definitions and restrictions on the classifier variables, refer to the Chapter 14, “Classifiers” in the *AT-S63 Management Software Menus Interface User’s Guide.*

Examples

This command creates a classifier for all IP traffic:

```
create classifier=4 description=”IP flow” protocol=ip
```

This command creates a classifier for all traffic originating from the subnet 149.22.22.0 destined to the device with the IP address 149.44.44.11:

```
create classifier=4 description=”subnet flow”
ipsaddr=149.22.22.0/24 ipdaddr=149.44.44.11
```

This command creates a classifier for all HTTPS web traffic with a destination IP address of 149.44.44.44:

```
create classifier=7 description=”HTTPS flow”
ipdaddr=149.44.44.44 tcpdport=443
```

DESTROY CLASSIFIER

Syntax

```
destroy classifier=idnumber
```

Parameters

classifier	Specifies the ID number of the classifier to be deleted. The number can be from 1 to 9999. You can delete more than one classifier at a time. You can specify the classifiers individually (e.g., 2,5,7) as a range (e.g., 11-14), or both (e.g., 2,4-8,12).

Description

This command deletes a classifier from the switch. To delete a classifier, you need to know its ID number. To display the ID numbers of the classifiers, refer to “SHOW CLASSIFIER” on page 287.

You cannot delete a classifier if it is assigned to an ACL or QoS policy. You must remove the classifier from the ACL or policy before you can delete it.

Example

This command deletes classifiers 2 and 4:

```
destroy classifier=2,4
```

PURGE CLASSIFIER

Syntax

```
purge classifier
```

Parameters

None.

Description

This command deletes all classifiers from the switch. You cannot delete the classifier if they are assigned to an ACL or QoS policy. You must first remove the classifiers from the ACL and policies before you can delete them.

Example

This command deletes all classifiers on the switch:

```
purge classifier
```

SET CLASSIFIER

Syntax

```
set classifier=idnumber [description="string"]
[macdaddr=macaddress|any] [macsaddr=macaddress|any]
[priority=value] [vlan=name|1..4094|any]
[protocol=ip|arp|rarp|number|any] [iptos=value|any]
[ipdscp=value|any] [ipprotocol=protocol|number|any]
[ipdaddr=ipaddress/mask|any] [ipsaddr=ipaddress/
mask|any] [tcpsport=value|any] [tcpdport=value|any]
[udpsport=value|any] [udpdport=value|any]
[tcpflags=[urg|ack|psh|rst|syn|fin|any]
```

Parameters

classifier	Specifies the ID number of the classifier to be modified. You can modify only one classifier at a time. The number can be from 1 to 9999.
description	Specifies a description of the classifier. A description can be up to fifteen alphanumeric characters. Spaces are allowed. If it contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.
macdaddr	Specifies a destination MAC address. The address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx
macsaddr	Specifies a source MAC address. The address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx
priority	Specifies the user priority level in a tagged Ethernet frame. The value can be 0 to 7.
vlan	Specifies a tagged or port-based VLAN by its name or VID number.
protocol	Specifies a Layer 2 protocol. Options are: IP ARP RARP You can specify additional Layer 2 protocols by entering the protocol number in either decimal or hexadecimal format. For the latter, precede the number with “0x”.

iptos	Specifies a Type of Service value. The range is 0 to 7.
ipdscp	Specifies a DSCP value. The range is 0 to 63.
ipprotocol	Specifies a Layer 3 protocol. Options are: TCP UDP ICMP IGMP You can specify other Layer 3 protocols by entering the protocol number in either decimal or hexadecimal format. If you use the latter, precede the number with "0x".
ipdaddr	Specifies a destination IP address. The address can be of a specific node or a subnet. To filter using the IP address of a subnet, you must include a mask. A mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the Class C subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits that represent the network section of the address. The address and mask are separated by a slash (/); for example, "IPDADDTR=149.11.11.0/24". No mask is necessary for the IP address of a specific end node.
ipsaddr	Specifies a source IP address. The address can be of a specific node or a subnet. If the latter, a mask must be included to indicate the subnet portion of the address. For an explanation of the mask, refer to the IPDADDR parameter.
tcpsport	Specifies a source TCP port.
tcpdport	Specifies a destination TCP port.
udpsport	Specifies a source UDP port.
udpdport	Specifies a destination UDP port.
tcpflags	Specifies a TCP flag. Options are URG - Urgent ACK - Acknowledgement RST - Reset PSH - Push SYN - Synchronization FIN - Finish

Description

This command modifies an existing classifier. The only setting of a classifier you cannot change is its ID number.

Specifying a new value for a variable that already has a value overwrites the current value with the new one. The ANY option removes a variable's value without assigning it a new value.

You cannot modify a classifier if it belongs to an ACL or QoS policy that is assigned to a port. You must first remove the port assignments from the ACL or policy before you can modify the it.

Examples

This command adds the destination IP address 149.22.22.22 and the source subnet IP address 149.44.44.0 to classifier ID 4:

```
set classifier=4 ipdaddr=149.22.22.22
ipsaddr=149.44.44.0/24
```

This command adds the Layer 3 protocol IGMP to classifier ID 6:

```
set classifier=6 ipprotocol=igmp
```

This command removes the current setting for the UDP destination port variable from classifier ID 5 without assigning a new value:

```
set classifier=5 udpdport=any
```

SHOW CLASSIFIER

Syntax

```
show classifier[=idnumber]
```

Parameters

classifier — Specifies the ID of the classifier you want to view. You can specify more than one classifier at a time.

Description

This command displays the classifiers on a switch. Figure 32 is an example of the information displayed by this command.

```
-----------------------------------------
Classifier ID: ................. 1
Description: ................... IP traffic
Protocol: ...................... 0x800 (IP)
Number of References: ........... 4
Number of Active Associations: .. 3
-----------------------------------------
Classifier ID: ................. 2
Description: ................... subnet 214
Dst IP/Mask: ................... 169.254.44.214
Number of References: ........... 1
Number of Active Associations: .. 1
-----------------------------------------
```

Figure 32. SHOW CLASSIFIER Command

The information displayed by this command is described here:

- ID - The classifier's ID number.
- Description - The description of the classifier.
- The Description is followed by the parameter settings of the classifier. Only those parameters that have been assigned a value are displayed. For an explanation of the parameters, refer to "CREATE CLASSIFIER" on page 278 or "SET CLASSIFIER" on page 284.
- Number of References - The number of active and inactive ACL and QoS policy assignments where the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one switch port while an inactive ACL or policy is not assigned to any ports. If this number is 0 (zero), the classifier has not been assigned to any ACLs or policies.

- Number of Active Associations - The number of active ACLs and QoS policy assignments where the classifier is currently assigned. An active ACL or policy is assigned to at least one switch port.

  You can use this number together with the Number of References to determine the number of inactive ACLs and policies for a classifier. For example, if Number of References for a classifier is 4 and the Number of Active Associations is 3, one of the ACL or QoS policy assignments for the classifier is not assigned to a switch port.

Examples

This command displays all of the classifiers on the switch:

```
show classifier
```

This command displays the details for just classifier ID 12:

```
show classifier=12
```

Chapter 18

Access Control List Commands

This chapter contains the following commands:

- “CREATE ACL” on page 290
- “DESTROY ACL” on page 292
- “PURGE ACL” on page 293
- “SET ACL” on page 294
- “SHOW ACL” on page 296

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 15, “Access Control Lists” in the *AT-S63 Management Software Menus Interface User’s Guide*.

CREATE ACL

Syntax

```
create acl=value [description="string"]
[action=deny|permit] classifierlist=value
[portlist=ports]
```

Parameters

acl — Specifies an ID number for the ACL. The number can be from 0 to 255. Each ACL must have a unique ID number.

description — Specifies a description for the ACL. A description can be up to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

action — Specifies the action to be taken by the port when a ingress packet matches a classifier attached to the ACL. Options are:

- permit — The port accepts the packet.
- deny — The port discards the packet, provided that the packet does not match the classifier of a permit ACL assigned to the same port. This is the default action.

classifierlist — Specifies the ID numbers of the classifiers to be assigned to the ACL. When entering multiple ID numbers, separate the numbers with a comma (e.g., 4,6,7). The classifiers must already exist on the switch. The order in which you specify the classifiers is not important. An ACL must have at least one classifier.

portlist — Specifies the port where this ACL is to be assigned. You can assign an ACL to more than one port. When entering multiple ports, the ports can be listed individually (e.g., 2,5,7), as a range (e.g., 8-12) or both (e.g., 1-4,6,8).

Description

This command creates an ACL. An ACL is used to filter ingress packets on a port.

Examples

The following command creates an ACL that discards the ingress traffic flow specified in classifier ID 18 and applies the ACL to port 4:

```
create acl=12 description=”IP flow deny” action=deny
classifierlist=18 portlist=4
```

The following command creates an ACL that discards the ingress traffic flows specified in classifier ID 2 and 17 and applies the ACL to ports 2 and 6:

```
create acl=6 description=”subnet flow deny”
action=deny classifierlist=2,17 portlist=2,6
```

The following command creates an ACL that permits the ingress traffic flow specified in classifier ID 18 and applies the ACL to ports 8 to 10:

```
create acl=24 description=”subnet flow deny”
action=permit classifierlist=18 portlist=8-10
```

DESTROY ACL

Syntax

```
destroy acl=value
```

Parameters

acl	Specifies ID number of the ACL you want to delete. You can delete more than ACL at a time.

Description

This command deletes an ACL from the switch.

Example

The following command deletes ACL IDs 14 and 17:

```
destroy acl=14,17
```

PURGE ACL

Syntax

```
purge acl
```

Parameters

None.

Description

This command deletes all ACLs on the switch.

Example

This command deletes all ACLs on the switch:

```
purge acl
```

SET ACL

Syntax

```
set acl=value [description=string]
[action=deny|permit] [classifierlist=value]
[portlist=ports|none]
```

Parameters

acl	Specifies the ID number of the ACL you want to modify. The number can be from 0 to 255. You can modify only one ACL at a time.
description	Specifies a new description for the ACL. A description can be up to 15 alphanumeric characters. Spaces are allowed. If the description contains a space, it must be enclosed in double quotes. Otherwise, the quotes are optional.
action	Specifies the new action to be taken by the port when an ingress packet matches a classifier attached to the ACL. Options are: permit — The port accepts the packet. deny — The port discards the packet, provided that the packet does not match the classifier of a permit ACL assigned to the same port.
classifierlist	Specifies the new ID numbers of the classifiers to be assigned to the ACL. Any classifier IDs already assigned to the ACL are overwritten. When entering multiple ID numbers, separate the numbers with a comma (e.g., 4,6,7). The classifiers must already exist on the switch. The order in which you specify the classifiers is not important. An ACL must be assigned at least one classifier.
portlist	Specifies the new ports to be assigned this ACL. Any ports to which the ACL is assigned are overwritten. You can assign an ACL to more than one port. When entering multiple ports, the ports can be listed individually (e.g., 2,5,7), as a range (e.g., 8-12) or both (e.g., 1-4,6,8). Entering NONE removes all ports to which the ACL is already assigned without assigning any new ports. An ACL without assigned ports exists, but remains nonfunctional until assigned to a port.

Description

This command modifies an ACL. You can use the command to change the description, action, classifiers, and ports of an ACL.

Examples

This command changes the description of ACL ID 4:

```
set acl=4 description=”ARP flow”
```

This command changes the action of ACL ID 6 to permit and reassigns it to ports 4 to 7:

```
set acl=6 action=permit portlist=4-7
```

This command changes the classifiers of ACL ID 41:

```
set acl=41 classifierlist=22,24,36
```

SHOW ACL

Syntax

show acl[=*id_number*]

Parameters

acl	Specifies the ID number of the ACL you want to view. You can specify more than one ACL at a time.

Description

This command displays the ACLs on the switch. An example of the information displayed by this command is shown in Figure 33.

```
-------------------------------------------
ACL ID ............. 1
Description ......... IP
Action .............. Deny
Classifier List ..... 1
Port List ........... 2-3
Is Active ........... Yes
-------------------------------------------
ACL ID ............. 2
Description ......... Subnets 211, 214
Action .............. Permit
Classifier List ..... 2,3
Port List ........... 2
Is Active ........... Yes
-------------------------------------------
ACL ID ............. 3
Description ......... Subnet 211
Action .............. Permit
Classifier List ..... 3
Port List ...........
Is Active ........... No
-------------------------------------------
```

Figure 33. SHOW ACL Command

The command displays the following information:

- ACL ID - The ACL's ID number.
- Description - The description of the ACL.
- Action - The action of the ACL. An active of Permit means that the port(s) where the ACL is assigned accepts those packets that meet the criteria of the classifiers. An action of Deny means that the port(s)

discards the packets provided that the packets do not also meet the criteria of a classifier of a Permit ACL assigned to the same port.

- Classifier List - The classifiers assigned to the ACL.
- Port List - The ports where the ACL is assigned.
- Is Active - The status of the ACL. An ACL is active if it is assigned to at least one port, and inactive if it is not assigned to any ports.

Examples

This command displays all of the ACLs on the switch:

```
show acl
```

This command displays ACL ID 22:

```
show acl=22
```

Chapter 19

Class of Service (CoS) Commands

This chapter contains the following commands:

- “MAP QOS COSP” on page 300
- “PURGE QOS” on page 302
- “SET QOS COSP” on page 303
- “SET QOS SCHEDULING” on page 304
- “SET SWITCH PORT PRIORITY OVERRIDEPRIORITY” on page 305
- “SHOW QOS CONFIG” on page 307

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 16, “Class of Service” in the *AT-S63 Management Software Menus Interface User’s Guide*.

MAP QOS COSP

Syntax

`map qos cosp=`*`priority-number`* `qid=`*`queue-number`*

Parameters

cosp — Specifies a Class of Service (CoS) priority level. The CoS priority levels are 0 through 7, with 0 as the lowest priority and 7 as the highest. You can specify more than one priority to assign to the same egress queue.

qid — Specifies the egress queue number. The egress queues are numbered 0 through 7, with queue 0 as the lowest priority and 7 as the highest.

Description

This command maps CoS priorities to port egress queues. You must specify both the priority and the queue ID. You can specify more than one priority to assign to the same egress queue. Table 11 lists the default mappings between the eight CoS priority levels and the eight egress queues of a switch port.

Table 11. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q1
1	Q0 (lowest)
2	Q2
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7 (highest)

Example

The following command maps priorities 4 and 5, to queue 3:

```
map qos cosp=4,5 qid=3
```

Equivalent Command

`set qos cosp=`*`priority-number`* `qid=`*`queue-number`*

For information, see "SET QOS COSP" on page 303.

PURGE QOS

Syntax

```
purge qos
```

Parameters

None

Description

This command destroys all policies, traffic classes, and flow groups; resets the CoS priorities to port egress queues to the default values; and sets the scheduling mode and egress weight queues to their default values.

Example

The following command resets QoS to the default values:

```
purge qos
```

SET QOS COSP

Syntax

`set qos cosp=`*`priority-number`* `qid=`*`queue-number`*

Parameters

cosp	Specifies a Class of Service (CoS) priority level. The CoS priority levels are 0 through 7, with 0 as the lowest priority and 7 as the highest. You can specify more than one priority to assign to the same egress queue.
qid	Specifies the egress queue number. The egress queues are numbered 0 through 7, with queue 0 as the lowest priority and 7 as the highest.

Description

This command maps CoS priorities to port egress queues. You must specify both the priority and the queue ID. You can assign more than one priority to an egress queue. Table 11 on page 300 lists the default mappings between the eight CoS priority levels and the eight egress queues of a switch port.

Example

The following command maps priorities 5 and 6 to egress queue 1:

```
set qos cosp=5,6 qid=1
```

Equivalent Command

`map qos cosp=`*`priority-number`* `qid=`*`queue-number`*

For information, see "MAP QOS COSP" on page 300.

SET QOS SCHEDULING

Syntax

```
set qos scheduling=strict|wrr weights=weights
```

Parameters

scheduling — Specifies the type of scheduling. The options are:

- strict — Strict priority. The port transmits all packets out of the higher priority queues before it transmits any from the low priority queues. This is the default.
- wrr — Weighted round robin. The port transmits a set number of packets from each queue in a round robin manner.

weights — Specifies the weight given to each of a port's eight egress priority queues. You must specify the weights if scheduling will be weighted round robin. The range for each queue is 1 to 15 packets, and the default is 1. The weights are specified in the following order: Q0, Q1, Q2, Q3, Q4, Q5, Q6, Q7. For example, to assign Q0 and Q1 a weight of 1, Q2 and Q3 a weight of 5, Q4 and Q5 a weight of 10, and Q6 and Q7 a weight of 15, you enter this parameter as `weights=1,1,5,5,10,10,15,15`. The parameter must include all eight queues.

Description

Sets the QoS scheduling method and the weights for round robin scheduling.

Examples

The following command sets the scheduling to strict:

```
set qos scheduling=strict
```

The following command sets the scheduling to weighted round robin and gives egress priority queues Q0 to Q3 a weight of 1, and Q4 to Q7 a weight of 15:

```
set qos scheduling=wrr weights=1,1,1,1,15,15,15,15
```

SET SWITCH PORT PRIORITY OVERRIDEPRIORITY

Syntax

```
set switch port=port [priority=value]
[overridepriority=yes|no|on|off|true|false]
```

Parameters

port	Specifies the port you want to configure. You can specify more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).
priority	Specifies a temporary priority level for all ingress untagged packets received on the port. If you include the OVERRIDEPRIORITY parameter, the temporary priority level will also apply to all ingress tagged packets. The range is 0 to 7; 0 is the lowest priority, and 7 is the highest. The default is 0.Table 11 on page 300 lists the default mappings between the priority levels and the egress queues:
overridepriority	Determines if a port should ignore the priority level in tagged packets and instead use the temporary priority level assigned to the port with the PRIORITY parameter. The options are:

yes, on, true	Overrides the priority level in tagged packets and uses the temporary priority level. This is the default. The options are equivalent.
no, off, false	Does not override the priority in tagged packets. The options are equivalent.

Description

This command can change a port's temporary priority level. It can also be used to determine whether a port receiving tagged packets should use the priority level in the frames or instead use a temporary priority level assigned to the port.

This command allows you to override the priority level mappings at the port level by assigning the packets a temporary priority. Note that this assignment is made when a packet is received on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port.

For example, you can configure a switch port so that all ingress frames are assigned a temporary priority level of 5, regardless of the actual priority levels that might be in the frames themselves, as found in tagged frames.

A temporary priority level applies only while a frame traverses the switching matrix. Tagged frames, which can contain a priority level, leave the switch with the same priority level they had when they entered the switch.

Examples

The following command changes the temporary priority level on ports 5, 8, and 12 to 5:

```
set switch port=5,8,12 priority=5
```

The following command activates the priority override feature on port 6 so that all ingress tagged packets use the port's temporary priority level:

```
set switch port=6 overridepriority=yes
```

SHOW QOS CONFIG

Syntax

```
show qos config
```

Parameters

None.

Description

Displays the CoS priority queues and scheduling. Figure 34 is an example of the information displayed by this command.

```
QoS Configuration information:

Number of CoS Queues .......... 8

CoS 0 Priority Queue .......... Q1
CoS 1 Priority Queue .......... Q0
CoS 2 Priority Queue .......... Q2
CoS 3 Priority Queue .......... Q3
CoS 4 Priority Queue .......... Q4
CoS 5 Priority Queue .......... Q5
CoS 6 Priority Queue .......... Q6
CoS 7 Priority Queue .......... Q7


Scheduling Mode ............... Strict Priority
Queue 0 Weight ................ 0
Queue 1 Weight ................ 0
Queue 2 Weight ................ 0
Queue 3 Weight ................ 0
Queue 4 Weight ................ 0
Queue 5 Weight ................ 0
Queue 6 Weight ................ 0
Queue 7 Weight ................ 0
```

Figure 34. SHOW QOS CONFIG Command

The current mapping of CoS priorities to port egress queues is displayed in the top section. As an example, at the default setting packets with a CoS priority of 3 are stored in egress queue 3 of a port.

The bottom section of the display shows the scheduling method of the switch ports. In strict priority, a port transmits all packets out of the higher priority queues before transmitting any from the low priority queues. This is the default. In weighted round robin, a port transmits a set number of packets from each queue. The weights only show a value when a port is

using weighted round robin and specify how many packets a port transmits from a queue before moving to the next queue.

Example

The following command displays the CoS priority queues and scheduling:

```
show qos config
```

Chapter 20

Quality of Service (QoS) Commands

This chapter contains the following commands:

- “ADD QOS FLOWGROUP” on page 310
- “ADD QOS POLICY” on page 311
- “ADD QOS TRAFFICCLASS” on page 312
- “CREATE QOS FLOWGROUP” on page 313
- “CREATE QOS POLICY” on page 316
- “CREATE QOS TRAFFICCLASS” on page 323
- “DELETE QOS FLOWGROUP” on page 328
- “DELETE QOS POLICY” on page 329
- “DELETE QOS TRAFFICCLASS” on page 330
- “DESTROY QOS FLOWGROUP” on page 331
- “DESTROY QOS POLICY” on page 332
- “DESTROY QOS TRAFFICCLASS” on page 333
- “PURGE QOS” on page 334
- “SET QOS FLOWGROUP” on page 335
- “SET QOS POLICY” on page 338
- “SET QOS PORT” on page 341
- “SET QOS TRAFFICCLASS” on page 342
- “SHOW QOS FLOWGROUP” on page 347
- “SHOW QOS POLICY” on page 349
- “SHOW QOS TRAFFICCLASS” on page 351

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to the Chapter 17, “Quality of Service,” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD QOS FLOWGROUP

Syntax

```
add qos flowgroup=value classifierlist=values
```

Parameter

flowgroup	Specifies the ID number of the flow group you want to modify. You can modify only one flow group at a time.
classifierlist	Specifies the new classifiers for the flow group. The new classifiers are added to any classifiers already assigned to the flow group. Separate multiple classifiers with commas (e.g., 4,11,12).

Description

This command adds classifiers to an existing flow group. The classifiers must already exist. Any classifiers already assigned to the flow group are retained by the group. If you want to add classifiers while removing the those already assigned, refer to “SET QOS FLOWGROUP” on page 335.

Example

This command adds the classifiers 4 and 7 to flow group 12:

```
add qos flowgroup=12 classifierlist=4,7
```

ADD QOS POLICY

Syntax

```
add qos policy=value trafficclasslist=values
```

Parameter

policy	Specifies the ID number of the policy you want to modify. You can modify only one policy at a time.
trafficclasslist	Specifies the new traffic classes of the policy. Traffic classes already assigned to the policy are retained. Separate multiple traffic classes with commas (e.g., 4,11,12).

Description

This command adds traffic classes to an existing policy. The traffic classes must already exist. Any traffic classes already assigned to the policy are retained by the policy. To add traffic classes while removing those already assigned, refer to "SET QOS POLICY" on page 338.

Example

This command adds the traffic class 16 to policy 11:

```
add qos policy=11 trafficclasslist=16
```

ADD QOS TRAFFICCLASS

Syntax

```
add qos trafficclass=value flowgrouplist=values
```

Parameter

trafficclass	Specifies the ID number of the traffic class you want to modify. You can modify only one traffic class at a time.
flowgrouplist	Specifies the new flow groups of the traffic class. The new flow groups are added to any flow groups already assigned to the flow group. Separate multiple flow groups with commas (e.g., 4,11,12).

Description

This command adds flow groups to an existing traffic class. The flow groups must already exist. Any flow groups already assigned to the traffic class are retained by the class. If you want to add flow groups while removing those already assigned, refer to “SET QOS TRAFFICCLASS” on page 342.

Examples

This command adds flow group 21 to traffic class 17:

```
add qos trafficclass=17 flowgrouplist=21
```

CREATE QOS FLOWGROUP

Syntax

```
create qos flowgroup=value [description="string"]
[markvalue=value|none] [priority=value|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[classifierlist=values|none]
```

Parameters

flowgroup	Specifies an ID number for the flow group. Each flow group on the switch must have a unique number. The range is 0 to 1023. The default is 0. This parameter is required.
description	Specifies a description for the flow group. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. This parameter is optional, but recommended. Names can help you identify the groups on the switch. The description must be enclosed in double quotes if it contains spaces. Otherwise, the quotes are optional.
markvalue	Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. If the NONE option is used, the frame's current DSCP value is not overwritten. The default is NONE. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.
priority	Specifies a new user priority value for the packets. The range is 0 to 7. If you want packets to retain the new value when they exit the switch, use the REMARKPRIORITY parameter. If the NONE option is used, the frame's current priority value is not overridden. The default is NONE. A new priority can be set at both the flow group and traffic class levels. If it is set in both places, the value in the flow group overrides the value in the traffic class.

remarkpriority — Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter. This parameter is ignored if the PRIORITY parameter is omitted or set to NONE. Options are:

- yes, on, true — Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter.
- no, off, false — Does not replace the user priority value in the packets with the new value specified in with the PRIORITY parameter. This is the default.

tos — Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.
- no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.
- no, off, false — Does not replace the ToS priority field. This is the default.

classifierlist — Specifies the classifiers to be assigned to the flow group. Separate multiple classifiers with commas (e.g., 4,7,8). The classifiers must already exist.

Description

This command creates a new flow group.

> **Note**
> For examples of command sequences used to create entire QoS policies, refer to "CREATE QOS POLICY" on page 316.

Examples

This command creates a flow group with an ID of 10 and the description "VoIP flow". The flow group is assigned a priority level of 7 and defined by classifiers 15 and 17. In this example, the packets of the flow group leave the switch with the same priority level as when they entered. The new priority level is relevant only as the packets traverse the switch. To alter the packets so that they leave containing the new level, you would include the REMARKPRIORITY parameter:

```
create qos flowgroup=10 description="VoIP flow"
priority=7 classifierlist=15,17
```

This command creates a similar flow group as in the previous example. The REMARKPRIORITY parameter is added so that the tagged packets of the flow group leave the switch with the new priority level of 7:

```
create qos flowgroup=10 description="VoIP flow"
priority=7 remarkpriority=yes classifierlist=15,17
```

This command creates a flow group whose DSCP value is changed to 59. The MARKVALUE parameter overwrites the current DSCP value in the packets, meaning the packets leave the switch with the new value. The classifiers of the flow group are 3, 14, and 24:

```
create qos flowgroup=10 description="DSCP 59 flow"
markvalue=59 classifierlist=3,14,24
```

CREATE QOS POLICY

Syntax

```
create qos policy=value [description="string"]
[indscpoverwrite=value|none] [remarkindscp=all|none]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[movepriioritytotos=yes|no|on|off|true|false]
[sendtomirror=yes|no|on|off|true|false]
[trafficclasslist=values|none]
[redirectport=value|none]
[ingressport=port|all|none] [egressport=port|none]
```

Parameters

policy	Specifies an ID number for the policy. Each policy on the switch must be assigned a unique number. The range is 0 to 255. The default is 0. This parameter is required.
description	Specifies a description for the policy. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional. This parameter is optional, but recommended. Names can help you identify the policies on the switch.
indscpoverwrite	Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. If None is specified, the DSCP value in the packets is not changed. The default is None. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.
remarkindscp	Specifies whether the DSCP value in ingress packets is overwritten. If All is specified, all packets are remarked. If None is specified, the function is disabled. The default is None.
tos	Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.
- no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

movepriioritytotos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.
- no, off, false — Does not replace the ToS priority field. This is the default.

sendtomirror — Copies the traffic that meets the criteria of the classifiers to a destination mirror port. Options are:

- yes, on, true — Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by creating a port mirror, as explained in Chapter 12, "Port Mirroring Commands" on page 193.
- no, off, false — Does not copy the traffic to a destination mirror port. This is the default.

trafficclasslist — Specifies the traffic classes to be assigned to the policy. The specified traffic classes must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

redirectport — Specifies the port to which the classified traffic from the ingress ports is redirected. The options are:

- value — Specifies a port number.
- none — No redirect port specified.

ingressport	Specifies the ingress ports to which the policy is to be assigned. Ports can be identified individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22). A port can be an ingress port of only one policy at a time. If a port is already an ingress port of a policy, you must remove the port from its current policy assignment before adding it to another policy.
egressport	Specifies the egress port to which the policy is to be assigned. You can enter only one egress port. The egress port must be within the same port block as the ingress ports. On switches with 24 ports (plus uplinks), ports 1-26 form a port block. On switches with 48 ports (plus uplinks), ports 1-24 and 49 form one port block and ports 25-48 and 50 form a second port block. A port can be an egress port of only one policy at a time. If a port is already an egress port of a policy, you must remove the port from its current policy assignment before adding it to another policy.

Description

This command creates a new QoS policy.

Examples

This command creates a policy with an ID of 75 and the description “DB flow.” The policy is appointed the traffic classes 12 and 25 and is assigned to ingress port 5:

```
create qos policy=75 description=”DB flow”
trafficclasslist=12,25 ingressport=5
```

This command creates a policy with an ID of 23 and the description “Video.” The ID of the traffic class for the policy is 19. The DSCP value is replaced with the value 50 for all ingress packets of the traffic class. The policy is assigned to port 14:

```
create qos policy=23 description=video
indscpoverwrite=50 remarkindscp=all
trafficclasslist=19 ingressport=14
```

QoS Command Sequence Examples

Creating a QoS policy involves a command sequence that creates one or more classifiers, a flow group, a traffic class, and finally the policy. The following sections contain examples of the command sequences for different types of policies.

Example 1: Voice Application

Voice applications typically require a small bandwidth but it must be consistent. They are sensitive to latency (interpacket delay) and jitter (delivery delay). Voice applications can be set up to have the highest priority.

This example creates two policies that ensure low latency for all traffic sent by and destined to a voice application located on a node with the IP address 149.44.44.44. The policies raise the priority level of the packets to 7, the highest level. Policy 6 is for traffic from the application that enter the switch on port 1. Policy 11 is for traffic arriving on port 8 going to the application.

Policy 6 Commands:

```
create classifier=22 description=”VoIP flow”
ipsadddr=149.44.44.44

create qos flowgroup=14 description=”VoIP flow”
priority=7 classifierlist=22

create qos trafficclass=18 description=”VoIP flow”
flowgrouplist=14

create qos policy=6 description=”VoIP flow”
trafficclasslist=18 ingressport=1
```

Policy 11 Commands:

```
create classifier=23 description=”VoIP flow”
ipdadddr=149.44.44.44

create qos flowgroup=17 description=”VoIP flow”
priority=7 classifierlist=23

create qos trafficclass=15 description=”VoIP flow”
flowgrouplist=17

create qos policy=11 description=”VoIP flow”
trafficclasslist=15 ingressport=8
```

The parts of the policies are:

- Classifiers - Define the traffic flow by specifying the IP address of the node with the voice application. The classifier for Policy 6 specifies the address as a source address since this classifier is part of a policy concerning packets coming from the application. The classifier for Policy 11 specifies the address as a destination address since this classifier is part of a policy concerning packets going to the application.
- Flow Groups - Specify the new priority level of 7 for the packets. It should be noted that in this example the packets leave the switch with the same priority level they had when they entered. The new priority level is relevant only as the packets traverse the switch. To alter the packets so that they leave containing the new level, you would use the REMARKPRIORITY option in the CREATE QOS FLOWGROUP command.
- Traffic Classes - No action is taken by the traffic classes, other than to specify the flow groups. Traffic class has a priority setting that can be used to override the priority level of packets, just as in a flow group. If you enter a priority value both in the flow group and the traffic class, the value in the flow group overrides the value in the traffic class.
- Policies - Specify the traffic class and the port to which the policy is to be assigned. Policy 6 is applied to port 1 since this is where the application is located. Policy 11 is applied to port 8 since this is where traffic going to the application will be received on the switch.

Example 2: Video Application

Video applications typically require a larger bandwidth than voice applications. Video applications can be set up to have a high priority and buffering, depending on the application.

This example creates policies with low latency and jitter for video streams (for example, net conference calls). The policies assign the packets a priority level of 4. The policies also limit the bandwidth for the video streams to 5 Mbps to illustrate how you can combine a change to the priority level with bandwidth restriction to further define traffic control. The node containing the application has the IP address 149.44.44.44. Policy 17 is assigned to port 1, where the application is located, and Policy 32 is assigned to port 8 where packets destined to the application enter the switch.

Policy 17 Commands:

```
create classifier=16 description=”video flow”
ipsadddr=149.44.44.44

create qos flowgroup=41 description=”video flow”
priority=4 classifierlist=16
```

```
create qos trafficclass=19 description=”video flow”
maxbandwidth=5 flowgrouplist=41

create qos policy=17 description=”video flow”
trafficclasslist=19 ingressport=1
```

Policy 32 Commands:

```
create classifier=42 description=”video flow”
ipdadddr=149.44.44.44

create qos flowgroup=36 description=”video flow”
priority=4 classifierlist=42

create qos trafficclass=21 description=”video flow”
maxbandwidth=5 flowgrouplist=36

create qos policy=32 description=”video flow”
trafficclasslist=21 ingressport=8
```

The parts of the policies are:

- Classifiers - Specify the IP address of the node with a video application. The classifier for Policy 17 specifies the address as a source address since this classifier is part of a policy concerning packets sent by the application. The classifier for Policy 32 specifies the address as a destination address since this classifier is part of a policy concerning packets going to the application.
- Flow Groups - Specify the new priority level of 4 for the packets. As with the previous example, the packets leave the switch with the same priority level they had when they entered. The new priority level is relevant only while the packets traverse the switch. To alter the packets so that they leave containing the new level, you would change option 5, Remark Priority, to Yes.
- Traffic Classes - Specify a maximum bandwidth of 5 Mbps for the packet stream. Bandwidth assignment can only be made at the traffic class level.
- Policies - Specify the traffic class and the port where the policy is to be assigned.

Example 3: Critical Database

Critical databases typically require a high bandwidth. They also typically require less priority than either voice or video.

The policies in this example assign 50 Mbps of bandwidth, with no change to priority, to traffic going to and from a database. The database is located on a node with the IP address 149.44.44.44 on port 1 of the switch.

Policy 15 Commands:

```
create classifier=42 description=database
ipsadddr=149.44.44.44

create qos flowgroup=36 description=database
classifierlist=42

create qos trafficclass=21 description=database
maxbandwidth=50 flowgrouplist=36

create qos policy=15 description=database
trafficclasslist=21 ingressport=1
```

Policy 17 Commands:

```
create classifier=10 description=database
ipdadddr=149.44.44.44

create qos flowgroup=12 description=database
classifierlist=10

create qos trafficclass=17 description=database
maxbandwidth=50 flowgrouplist=12

create qos policy=17 description=database
trafficclasslist=17 ingressport=8
```

CREATE QOS TRAFFICCLASS

Syntax

```
create qos trafficclass=value [description="string"]
[exceedaction=drop|remark]
[exceedremarkvalue=value|none] [markvalue=value|none]
[maxbandwidth=value|none] [burstsize=value|none]
[priority=value|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[movepriioritytotos=yes|no|on|off|true|false]
[flowgrouplist=values|none]
```

Parameters

trafficclass	Specifies an ID number for the flow group. Each flow group on the switch must be assigned a unique number. The range is 0 to 511. The default is 0. This parameter is required.
description	Specifies a description for the traffic class. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. This parameter is optional, but recommended. Names can help you identify the traffic classes on the switch.
exceedaction	Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth, specified with the MAXBANDWIDTH parameter. There are two possible exceed actions, drop and remark. If drop is selected, traffic exceeding the bandwidth is discarded. If remark is selected, the packets are forwarded after replacing the DSCP value with the new value specified in option 4, Exceed Remark Value. The default is drop.
exceedremarkvalue	Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value set with the MARKVALUE parameter. The range is 0 to 63. The default is 0.
markvalue	Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

	A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.
maxbandwidth	Specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum rate at which the ingress port accepts data belonging to this traffic class before either dropping or remarking occurs, depending on the EXCEEDACTION parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified. The range is 0 to 1016 Mbps. The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16).
burstsize	Specifies the size of a token bucket for the traffic class. The token bucket is used in situations where you have set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded. Tokens are added to the bucket at the same rate as the traffic class' maximum bandwidth, set with the MAXBANDWIDTH parameter. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at that rate. If the amount of the traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic will be discarded since no tokens are available for handling the increase.

If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded.

Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added. The range is 4 to 512 Kbps.

This parameter must be used with the MAXBANDWIDTH parameter. Specifying a token bucket size without also specifying a maximum bandwidth serves no function.

priority

Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of eight Class of Service (CoS) queues based on the priority value.

If you want the packets to retain the new value when they exit the switch, use the REMARKPRIORITY parameter.

A new priority can be set at both the flow group and traffic class levels. If it is set in both places, the value in the flow group overrides the value in the traffic class.

remarkpriority

Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter. This parameter is ignored if the PRIORITY parameter is omitted or set to NONE. Options are:

yes, on, true — Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter.

no, off, false — Does not replace the user priority value in the packets with the new value specified in with the PRIORITY

parameter. This is the default.

tos	Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.
movetostopriority	Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are: yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. no, off, false — Does not replace the preexisting 802.1p priority level This is the default.
movepriioritytotos	Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are: yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. no, off, false — Does not replace the ToS priority field. This is the default.
flowgrouplist	Specifies the flow groups to be assigned to the traffic class. The specified flow groups must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

Description

This command creates a new traffic class.

Note
For examples of command sequences used to create entire QoS policies, refer to “CREATE QOS POLICY” on page 316.

Examples

The following command creates a traffic class with an ID number of 25 and the description "Database flow". The only parameter in the traffic class is the identification of the flow group, which is 11:

```
create qos trafficclass=25 description="Database flow"
flowgrouplist=11
```

This command creates a traffic class with the ID number of 41 and description "Video flow". The traffic class is assigned the flow group 3 and is given a maximum bandwidth of 5 Mbps:

```
create qos trafficclass=41 description="Video flow"
maxbandwidth=5 flowgrouplist=3
```

This command creates a traffic class with the ID number of 51 and description "DB Eng". It assigns flow group 5 a maximum bandwidth of 50 Mbps. The DSCP value in all flow traffic that exceeds the maximum bandwidth is changed to 35:

```
create qos trafficclass=51 description="DB Eng"
exceedaction=remark exceedremarkvalue=35
maxbandwidth=50 flowgrouplist=5
```

DELETE QOS FLOWGROUP

Syntax

```
delete qos flowgroup=value classifierlist=values
```

Parameter

flowgroup	Specifies the ID number of the flow group you want to modify. You can modify only one flow group at a time.
classifierlist	Specifies the classifiers you want to remove from the flow group. Separate multiple classifiers with commas (e.g., 4,11,12). (The online help for this command includes a NONE option for this parameter. Specifying the NONE option does not remove any classifiers. Since the purpose of this command is to remove classifiers from a flow group, it is unlikely you would ever use that option.)

Description

This command removes classifiers from a flow group.

Example

This command removes classifier 6 from flow group 22:

```
delete qos flowgroup=22 classifierlist=6
```

DELETE QOS POLICY

Syntax

```
delete qos policy=value trafficclasslist=values
```

Parameter

policy	Specifies the ID number of the policy you want to modify. You can modify only one policy at a time.
trafficclasslist	Specifies the IDs of the traffic classes you want to remove from the policy. Separate multiple traffic class with commas (e.g., 4,11,12). (The online help for this command includes a NONE option for this parameter. Specifying the NONE option does not remove any traffic classes. Since the purpose of this command is to remove traffic classes from a policy, it is unlikely you would ever use that option.)

Description

This command removes traffic classes from policies.

Example

This command removes traffic class 17 from policy 1:

```
delete qos policy=1 trafficclasslist=17
```

DELETE QOS TRAFFICCLASS

Syntax

```
delete qos trafficclass=value flowgrouplist=values
```

Parameter

flowgroup	Specifies the ID number of the traffic class you want to modify. You can modify only one traffic class at a time.
flowgrouplist	Specifies the IDs of the flow groups you want to remove from the traffic class. Separate multiple flow groups with commas (e.g., 4,11,12). (The online help for this command includes a NONE option for this parameter. Specifying the NONE option does not remove any flow groups. Since the purpose of this command is to remove flow groups from a traffic class, it is unlikely you would ever use that option.)

Description

This command removes flow groups from traffic classes.

Example

This command removes flow group 5 from traffic class 22:

```
delete qos trafficclass=22 flowgrouplist=5
```

DESTROY QOS FLOWGROUP

Syntax

```
destroy qos flowgroup=value
```

Parameter

flowgroup — Specifies the ID number of the flow group you want to delete. You can delete more than one flow group at a time. You can specify the flow groups individually, as a range, or both.

Description

This command deletes flow groups.

Examples

This command deletes the flow group 22:

```
destroy qos flowgroup=22
```

This command deletes the flow groups 16 to 20 and 23:

```
destroy qos flowgroup=16-20,23
```

DESTROY QOS POLICY

Syntax

```
destroy qos policy=value
```

Parameter

flowgroup	Specifies the ID number of the policy you want to delete. You can delete more than one policy at a time. You can specify the flow groups individually, as a range, or both.

Description

This command deletes QoS policies.

Examples

This command deletes policy 41:

```
destroy qos policy=41
```

This command deletes policies 5 and 23:

```
destroy qos policy=5,23
```

DESTROY QOS TRAFFICCLASS

Syntax

```
destroy qos trafficclass=value
```

Parameter

trafficclass — Specifies the ID number of the traffic class you want to delete. You can delete more than one traffic class at a time. You can specify the flow groups individually, as a range, or both.

Description

This command deletes traffic classes.

Examples

This command deletes traffic class 22:

```
destroy qos trafficclass=22
```

This command deletes traffic classes 16 to 20 and 23:

```
destroy qos trafficclass=16-20,23
```

PURGE QOS

Syntax

```
purge qos
```

Parameters

None

Description

This command destroys all policies, traffic classes, and flow groups; resets the CoS priorities to port egress queues to the default values; and sets the scheduling mode and egress weight queues to their default values.

Example

The following command resets QoS to the default values:

```
purge qos
```

SET QOS FLOWGROUP

Syntax

```
set qos flowgroup=value [description=string]
[markvalue=value|none] [priority=value|NONE]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[movepriioritytotos=yes|no|on|off|true|false]
[classifierlist=values|none]
```

Parameters

flowgroup	Specifies the ID number of the flow group you want to modify. The range is 0 to 1023.
description	Specifies a new description for the flow group. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. This parameter is optional, but recommended. Names can help you identify the groups on the switch. The description must be enclosed in double quotes if it contains spaces. Otherwise, the quotes are optional.
markvalue	Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. If the NONE option is used, the frame's current DSCP value is not overwritten. The default is NONE. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.
priority	Specifies a new user priority value for the packets. The range is 0 to 7. You can specify only one value. If you want packets to retain the new value when they exit the switch, use the REMARKPRIORITY parameter. If the NONE option is used, the frame's current priority value is not overridden The default is NONE. If you specify a new priority in a flow group and a traffic class, the value in the flow group overrides the value in the traffic class.
remarkpriority	Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter. This parameter is ignored if the PRIORITY parameter is

omitted or set to NONE. Options are:

yes, on, true — Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter.

no, off, false — Does not replace the user priority value in the packets with the new value specified in with the PRIORITY parameter. This is the default.

tos — Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

movepriioritytotos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no, off, false — Does not replace the ToS priority field. This is the default.

classifierlist — Specifies the classifiers to be assigned to the flow group. The specified classifiers replace any classifiers already assigned to the flow group. Separate multiple classifiers with commas (e.g., 4,7,8). The classifiers must already exist. The NONE options removes all classifiers currently assigned to the flow group without assigning any new ones. To add classifiers without replacing those already assigned, see “ADD QOS FLOWGROUP” on page 310.

Description

This command modifies the specifications of an existing flow group. The only parameter you cannot change is a flow group's ID number. To initially create a flow group, refer to "CREATE QOS FLOWGROUP" on page 313.

> **Note**
> For examples of command sequences used to create entire QoS policies, refer to "CREATE QOS POLICY" on page 316.

When modifying a flow group, note the following:

- You cannot change a flow group's ID number.
- Specifying an invalid value for a parameter that already has a value causes the parameter to revert to its default value.

Examples

This command changes the user priority value to 6 in flow group 15:

```
set qos flowgroup=15 priority=6
```

This command assigns classifiers 23 and 41 to flow group 25. Any classifiers already assigned to the flow group are replaced:

```
set qos flowgroup=25 classifierlist=23,41
```

This command returns the MARKVALUE setting in flow group 41 back to the default setting of NONE. At this setting, the flow group will not overwrite the ToS setting in the packets:

```
set qos flowgroup=41 markvalue=none
```

SET QOS POLICY

Syntax

```
set qos policy=value [description=string]
[indscpoverwrite=value|none] [remarkindscp=[all|none]]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[movepriioritytotos=yes|no|on|off|true|false]
[sendtomirror=yes|no|on|off|true|false]
[trafficclasslist=values|none]
[redirectport=value|none] [ingressport=port|all|none]
[egressport=port|none]
```

Parameters

policy	Specifies an ID number for the policy. Each policy on the switch must be assigned a unique number. The range is 0 to 255. The default is 0. This parameter is required.
description	Specifies a description for the policy. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional. This parameter is optional, but recommended. Names can help you identify the policies on the switch.
indscpoverwrite	Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.
remarkindscp	Specifies the conditions under which the ingress DSCP value is overwritten. If All is specified, all packets are remarked. If None is specified, the function is disabled. The default is None.
tos	Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in

a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.
- no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.
- no, off, false — Does not replace the ToS priority field. This is the default.

sendtomirror — Copies the traffic that meets the criteria of the classifiers to a destination mirror port. Options are:

- yes, on, true — Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by creating a port mirror, as explained in Chapter 12, "Port Mirroring Commands" on page 193.
- no, off, false — Does not copy the traffic to a destination mirror port. This is the default.

trafficclasslist — Specifies the traffic classes to be assigned to the policy. The specified traffic classes must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

redirectport — Specifies the port to which the classified traffic from the ingress ports is redirected.

ingressport — Specifies the ingress ports to which the policy is to be assigned. Ports can be identified individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22). The NONE option removes the policy from all ingress ports to which it has been assigned. The ALL option adds it to all ports.

A port can be an ingress port of only one policy at a time. If a port is already an ingress port of a policy, you must remove the port from its current policy assignment before adding it to another policy. Alternatively, you can use "SET QOS PORT" on page 341, which removes a port from a policy and adds it to another policy with one command.

egressport — Specifies the egress port to which the policy is to be assigned. You can enter only one egress port. The NONE option removes the policy from all egress ports to which it has been assigned. The ALL option adds it to all ports.

A port can be an egress port of only one policy at a time. If a port is already an egress port of a policy, you must remove the port from its current policy assignment before adding it to another policy. Alternatively, you can use "SET QOS PORT" on page 341, which removes a port from a policy and adds it to another policy with one command.

Description

This command modifies an existing policy. To initially create a policy, refer to "CREATE QOS POLICY" on page 316.

Note
For examples of command sequences used to create entire QoS policies, refer to "CREATE QOS POLICY" on page 316.

When modifying a policy, note the following:

- You cannot change a policy's ID number.
- Specifying an invalid value for a parameter that already has a value causes the parameter to revert to its default value.

Examples

This command changes the ingress port for policy 8 to port 23:

```
set qos policy=8 ingressport=8
```

This command changes the traffic classes assigned to policy 41:

```
set qos policy=41 trafficclasslist=12,23
```

SET QOS PORT

Syntax

```
set qos port=value type=ingress|egress
policy=value|none
```

Parameter

port	Specifies the port to which the policy is to be assigned or removed. You can specify more than one port at a time if the port is an ingress port of the traffic flow. Ports can be identified individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22). You can specify only one port if the port is functioning as an egress port for the flow.
type	Specifies whether the port is an ingress or egress port for the traffic flow of the policy. The default is ingress.
policy	Specifies the policy to the assigned to the port. You can specify only one policy. The NONE option removes the currently assigned policy from a port.

Description

This command adds and removes ports from policies.

A port can be an ingress or egress port of only one policy at a time. However, a port can be an ingress port and an egress port of different policies, simultaneously. If a port is already a port of a policy, this command automatically removes it from its current policy assignment before adding it to another policy.

Examples

This command assigns QoS policy 12 to ingress ports 5 through 8:

```
set qos port=5-8 type=ingress policy=12
```

This command removes the currently assigned policy to egress ports 1 and 5:

```
set qos port=1,5 type=egress policy=none
```

SET QOS TRAFFICCLASS

Syntax

```
set qos trafficclass=value [description="string"]
[exceedaction=drop|remark]
[exceedremarkvalue=value|none] [markvalue=value|none]
[maxbandwidth=value|none] [burstsize=value|none]
[priority=value|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[movepriioritytotos=yes|no|on|off|true|false]
[flowgrouplist=values|none]
```

Parameters

trafficclass	Specifies an ID number for the flow group. Each flow group on the switch must be assigned a unique number. The range is 0 to 511. The default is 0. This parameter is required.
description	Specifies a description for the traffic class. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional. This parameter is optional, but recommended. Names can help you identify the traffic classes on the switch.
exceedaction	Specifies the action to be taken if the flow group of the traffic class exceeds the maximum bandwidth, specified with the MAXBANDWIDTH parameter. There are two possible exceed actions, drop and remark. If drop is selected, traffic exceeding the bandwidth is discarded. If remark is selected, the packets are forwarded after replacing the DSCP value with the new value specified with the EXCEEDREMARKVALUE parameter. The default is drop.
exceedremarkvalue	Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value set with the MARKVALUE parameter. The range is 0 to 63. The default is 0.

markvalue	Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.
maxbandwidth	Specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum rate at which the ingress port accepts data belonging to this traffic class before either dropping or remarking occurs, as specified with the EXCEEDACTION parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified. The range is 0 to 1016 Mbps. The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16).
burstsize	Specifies the size of a token bucket for the traffic class. The token bucket is used in situations where you have set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded. Tokens are added to the bucket at the same rate as the traffic class' maximum bandwidth, set with the MAXBANDWIDTH parameter. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at that rate. If the amount of the traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no

	unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic will be discarded since no tokens are available for handling the increase. If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded. Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added. The range is 4 to 512 Kbps. This parameter should be used with the MAXBANDWIDTH parameter. Specifying a token bucket size without also specifying a maximum bandwidth serves no function.
priority	Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of eight Class of Service (CoS) queues based on the priority value. If you want the packets to retain the new value when they exit the switch, change option 9, Remark Priority, to Yes. If you specify a new priority in a flow group and a traffic class, the value in the flow group overrides the value in the traffic class.
remarkpriority	Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter, if set to Yes. If set to No, which is the default, the packets retain their preexisting priority level when they leave the switch.
tos	Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.
- no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

movepriioritytotos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

- yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.
- no, off, false — Does not replace the ToS priority field. This is the default.

flowgrouplist — Specifies the flow groups to be assigned to the traffic class. Any flow groups already assigned to the traffic class are replaced. The specified flow groups must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

Description

This command modifies an existing traffic class. To initially create a traffic class, refer to "CREATE QOS TRAFFICCLASS" on page 323. The only parameter you cannot change is a traffic classes ID number.

Note
For examples of command sequences used to create entire QoS policies, refer to "CREATE QOS POLICY" on page 316.

When modifying a traffic class, note the following:

- You cannot change a traffic class' ID number.
- Specifying an invalid value for a parameter that already has a value causes the parameter to revert to its default value.

Examples

This command changes the exceed action in traffic class 18 to remark and specifies a remark value of 24. This command changes the DSCP value in traffic that exceeds the maximum bandwidth to 24:

```
set qos trafficclass=18 exceedaction=remark
exceedremarkvalue=24
```

This command changes the user priority value to 17 for traffic belonging to traffic class 42:

```
set qos trafficclass=42 priority=17
```

This command changes the maximum bandwidth for traffic class 41 to 80 Mbps and the burst size to 400 Kbps.

```
set qos trafficclass=41 maxbandwidth=80 burstsize=400
```

SHOW QOS FLOWGROUP

Syntax

show qos flowgroup[=*idnumber*]

Parameters

flowgroup Specifies the ID of the flow group you want to view. You can specify more than one classifier at a time.

Description

This command displays the flow groups on a switch. An example is shown in Figure 35.

```
Flow Group ID ............... 2
Description ................. Video1
DSCP value .................. 0
Priority .................... 6
Remark Priority ............. No
ToS ........................
Move ToS to Priority ....... No
Move Priority to ToS ....... No
Classifier List ............. 11
Parent Traffic Class ID .... 4
Is Active ................... Yes
```

Figure 35. SHOW QOS FLOWGROUP Command

The command displays the following information about a flow group:

- Flow Group ID - The flow group's ID number.
- Description - The flow group's description.
- DSCP value - The replacement value to write into the DSCP (TOS) field of the packets.
- Priority - The new user priority value for the packets.
- Remark Priority - Replaces the user priority value in the packets with the Priority value.
- ToS - Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.
- Move ToS to Priority - If set to Yes, replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting 802.1p priority level.
- Move Priority to ToS - If set to Yes, replaces the value in the ToS priority field with the value in the 802.1p priority field on IPv4 packets. If

set to No, which is the default, the packets retain their preexisting ToS priority level.

- Classifier List - The classifiers assigned to the policy.
- Parent Traffic Class ID - The ID number of the traffic class to which the flow group is assigned. A flow group can belong to only one traffic class at a time.
- Is Active - The status of the flow group. If the flow group is part of a QoS policy that is assigned to one or more ports, the flow group is deemed active. If the flow group has not been assigned to a policy or if the policy has not been assigned to any ports, the flow group is considered inactive.

For further information about the parameters, refer to “CREATE QOS FLOWGROUP” on page 313.

Examples

This command displays all of the flow groups:

```
show qos flowgroup
```

This command displays flow group 12:

```
show qos flowgroup=12
```

SHOW QOS POLICY

Syntax

```
show qos policy[=idnumber]
```

Parameter

policy — Specifies the ID of the policy you want to view. You can specify more than one policy at a time. Separate multiple policies with commas (e.g., 4,5,10).

Description

This command displays the policies on a switch. An example is shown in Figure 36.

```
Policy ID ................ 11
Description .............. policy_ca2
Remark DSCP .............. All
In DSCP overwrite ........ 42
ToS .......................
Move ToS to Priority ..... No
Move Priority to ToS ..... No
Send to Mirror Port ...... No
Traffic Class List .......
Redirect Port ............
Ingress Port List ........ 15
Egress Port ..............
Is Active ................ Yes
```

Figure 36. SHOW QOS POLICY Command

This command provides the following information:

- Policy ID - The policy's ID number.
- Description - The policy's description.
- Remark DSCP - Specifies whether the DSCP value of ingress packets is overwritten. If All is specified, all packets are remarked. If None is specified, the function is disabled. The default is None.
- In DSCP overwrite - The replacement value to write into the DSCP (TOS) field of the packets.
- ToS - Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. A ToS value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.
- Move ToS to Priority - If set to yes, replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting

802.1p priority level.

- Move Priority to ToS - If set to yes, replaces the value in the ToS priority field with the value in the 802.1p priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting ToS priority level.
- Send to Mirror Port - Copies the traffic that meets the criteria of the classifiers to a destination mirror port. If set to yes, you must specify the destination port of the port mirror with “SET SWITCH MIRROR” on page 194.
- Traffic Class List - The traffic classes assigned to the policy.
- Redirect Port - The egress port to which the classified traffic from the ingress port is reassigned.
- Ingress Port List - The ingress ports to which the policy is assigned.
- Egress Port - The egress port to which the policy is assigned.
- Active - The status of the policy. A policy that is assigned to one or more ports is deemed active while a policy that is not assigned to any ports is deemed inactive.

For further information about the parameters, refer to “CREATE QOS POLICY” on page 316.

Examples

This command displays all of the policies:

```
show qos policy
```

This command displays policy 54:

```
show qos policy=54
```

SHOW QOS TRAFFICCLASS

Syntax

```
show qos trafficclass[=idnumber]
```

Parameter

trafficclass — Specifies the ID of the traffic class you want to view. You can specify more than one traffic class at a time. Separate multiple traffic classes with commas (e.g., 4,5,10).

Description

This command displays the traffic classes on a switch. An example is shown in Figure 37.

```
Traffic Class ID ......... 0
Description ............... Dev Database
Exceed Action ............. Drop
Exceed Remark Value ....... 0
DSCP value ................ 0
Max bandwidth ............. 50
Burst Size ................ 0
Priority .................. 0
Remark Priority ........... No
ToS ........................
Move ToS to Priority ...... No
Move Priority to ToS ...... No
Flow Group List ........... 11
Parent Policy ID .......... 2
Is Active ................. Yes
```

Figure 37. DISPLAY QOS TRAFFICCLASS Command

This command provides the following information about a traffic class:

- Traffic Class ID - The traffic class' ID number.
- Description - The description of the traffic class.
- Exceed Action - The action taken if the traffic of the traffic class exceeds the maximum bandwidth.
- Exceed Remark Value - The DSCP replacement value for traffic that exceeds the maximum bandwidth.
- DSCP value - The replacement value to write into the DSCP (TOS) field of the packets.
- Max Bandwidth - The maximum bandwidth available to the traffic class.
- Burst Size - The size of a token bucket for the traffic class.

- Priority - The priority value in the IEEE 802.1p tag control field assigned to the traffic that belongs to this traffic class.
- Remark Priority - Replaces the user priority value in the packets with the Priority value.
- ToS - Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.
- Move ToS to Priority - If set to yes, replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting 802.1p priority level.
- Move Priority to ToS - If set to yes, replaces the value in the ToS priority field with the value in the 802.1p priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting ToS priority level.
- Flow Group List - The flow groups assigned to the traffic class.
- Parent Policy ID - The ID number of the policy where the traffic class is assigned. A traffic class can belong to only one policy at a time.
- Is Active - The status of the traffic class. If the traffic class is part of a QoS policy that is assigned to one or more ports, the traffic class is deemed active. If the traffic class has not been assigned to a policy or if the policy has not been assigned to any ports, the traffic class is deemed inactive.

For further information about the parameters, refer to “CREATE QOS TRAFFICCLASS” on page 323.

Examples

This command displays all of the traffic classes:

```
show qos trafficclass
```

This command displays traffic class 14:

```
show qos trafficclass=14
```

Chapter 21

Denial of Service Defense Commands

This chapter contains the following command:

- ❒ “SET DOS” on page 354
- ❒ “SET DOS IPOPTION” on page 355
- ❒ “SET DOS LAND” on page 357
- ❒ “SET DOS PINGOFDEATH” on page 358
- ❒ “SET DOS SMURF” on page 360
- ❒ “SET DOS SYNFLOOD” on page 361
- ❒ “SET DOS TEARDROP” on page 362
- ❒ “SHOW DOS” on page 364

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 18, “Denial of Service Defense” in the *AT-S63 Management Software Menus Interface User’s Guide*.

SET DOS

Syntax

```
set dos ipaddress=ipaddress subnet=mask uplinkport=port
```

Parameters

ipaddress	Specifies the IP address of one of the devices connected to the switch, preferably the lowest IP address.
subnet	Specifies the subnet mask of the LAN. A binary “1” indicates the switch should filter on the corresponding bit of the address, while a “0” indicates that it should not.
uplinkport	Specifies the port on the switch that is connected to a device (for example, a DSL router) that leads outside the network. You can specify only one port. This parameter is required only for the Land defense. The default port is the highest numbered existing port in the switch.

Description

This command is required for the SMURF and Land defenses. The SMURF defense uses the LAN address and mask to determine the broadcast address of your network. The Land defense uses this information to determine which traffic is local and which is remote to your network.

As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to 149.11.11.50. The IP address would be 149.11.11.1 and the mask would be 0.0.0.63.

Examples

The following command sets the IP address to 149.11.11.1 and the mask to 0.0.0.63:

```
set dos ipaddress=149.11.11.1 subnet=0.0.0.63
```

The following command sets the IP address to 149.22.22.1, the mask to 0.0.0.255, and the uplink port for the Land defense to port 24:

```
set dos ipaddress=149.22.22.1 subnet=0.0.0.255 uplinkport=24
```

SET DOS IPOPTION

Syntax

```
set dos ipoption port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port — Specifies the switch port where you want to enable or disable the IP Option defense. You can specify more than one port at a time.

state — Specifies the state of the IP Option defense. The options are:

- enable — Activates the defense.
- disable — Deactivates the defense. This is the default.

mirroring — Specifies whether the examined traffic is copied to a mirror port. Options are:

- yes, on, true enabled — Traffic is mirrored. These values are equivalent.
- no, off, false disabled — Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command enables and disables the IP Option DoS defense.

This type of attack occurs when an attacker sends packets containing bad IP options to a victim node. There are many different types of IP options attacks and the AT-S63 management software does not try to distinguish between them. Rather, a switch port where this defense is activated counts the number of ingress IP packets containing IP options. If the number exceeds 20 packets per second, the switch considers this a possible IP options attack and does the following occurs:

- The switch sends a trap to the management stations.
- The switch blocks all traffic on the port for one minute.

This defense mechanism does not involve the switch's CPU. You can activate it on as many ports as you want without it impacting switch performance.

You can use the MIRRORING parameter to copy the examined traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to “SET SWITCH MIRROR” on page 194.

Example

The following command activates the IP Options defense on ports 5, 7, and 10:

```
set dos ipoption port=5,7,10 state=enable
```

The following command activates the IP Options defense on port 6 as well as the mirroring feature so the examined traffic is copied to a destination port mirror.

```
set dos ipoption port=6 state=enable mirroring=yes
```

The following command disables the IP Options defense on ports 5 and 7:

```
set dos ipoption port=5,7 state=disable
```

SET DOS LAND

Syntax

```
set dos land port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port — Specifies the switch port on which you want to enable or disable the Land defense. You can specify more than one port at a time.

state — Specifies the state of the Land defense. The options are:

- enable — Activates the defense.
- disable — Deactivates the defense. This is the default.

mirroring — Specifies whether the examined traffic is copied to a mirror port. Options are:

- yes, on, true enabled — Traffic is mirrored. These values are equivalent.
- no, off, false disabled — Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command enables and disables the Land DoS defense. For an explanation of this attack and the AT-S63 defense mechanism, refer to Chapter 18, "Denial of Service Defense" in the *AT-S63 Management Software Menus Interface User's Guide*.

You can use the MIRRORING parameter to copy the intruding traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to "SET SWITCH MIRROR" on page 194.

Example

The following command activates the Land defense on ports 5 and 7:

```
set dos land port=5,7 state=enable
```

SET DOS PINGOFDEATH

Syntax

```
set dos pingofdeath port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port — Specifies the switch ports on which to enable or disable the Ping of Death defense. You can specify more than one port at a time.

state — Specifies the state of the IP Option defense. The options are:

- enable — Activates the defense.
- disable — Deactivates the defense. This is the default.

mirroring — Specifies whether the examined traffic is copied to a mirror port. Options are:

- yes, on, true enabled — Traffic is mirrored. These values are equivalent.
- no, off, false disabled — Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command activates and deactivates the Ping of Death DoS defense.

In this DoS, an attacker sends an oversized, fragmented Ping packet to the victim, which, if lacking a policy for handling oversized packets, may freeze.

To defend against this form of attack, a switch port searches for the last fragment of a fragmented Ping request and examines its offset to determine if the packet size is greater than 63,488 bits. If it is, the fragment is forwarded to the switch's CPU for final packet size determination. If the switch determines that the packet is oversized, the following occurs:

- The switch sends a trap to the management stations.
- The switch blocks all traffic on the port for one minute.

Note
This defense mechanism requires some involvement by the switch's CPU, though not as much as the Teardrop defense. This will not impact the forwarding of traffic between the switch ports, but it can affect the handling of CPU events, such as the processing of IGMP packets and spanning tree BPDUs. For this reason, Allied Telesyn recommends that you strictly limit the use of this defense, activating it only on those ports where an attack is most likely to originate.

You can use the MIRRORING parameter to copy the offending traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to "SET SWITCH MIRROR" on page 194.

Example

The following command activates the defense on ports 1 and 5:

```
set dos pingofdeath port=1,5 state=enable
```

SET DOS SMURF

Syntax

```
set dos smurf port=port state=enable|disable
```

Parameters

port — Specifies the switch ports on which you want to enable or disable SMURF defense. You can select more than one port at a time.

state — Specifies the state of the SMURF defense. The options are:

- enable — Activates the defense.
- disable — Deactivates the defense. This is the default.

Description

This command activates and deactivates the SMURF DoS defense.

This DoS attack is instigated by an attacker sending a Ping request containing a broadcast address as the destination address and the address of the victim as the source of the Ping. This overwhelms the victim with a large number of Ping replies from other network nodes.

A switch port defends against this form of attack by examining the destination addresses of ingress Ping packets and discarding those that contain a broadcast address as a destination address.

To implement this defense, you need to specify the IP address of any device on your network, preferably the lowest IP address, and a mask using “SET DOS” on page 354. The switch uses the combination of the two to determine your network’s broadcast address. Any ingress Ping packets containing the broadcast address are discarded.

This defense mechanism does not involve the switch’s CPU. You can activate it on as many ports as you want without having it negatively impact switch performance.

Example

The following command activates this defense on port 17:

```
set dos smurf port=17 state=enable
```

SET DOS SYNFLOOD

Syntax

```
set dos synflood port=port state=enable|disable
```

Parameters

port — Specifies the switch ports on which you want to enable or disable this DoS defense. You can select more than one port at a time.

state — Specifies the state of the DoS defense. The options are:

- enable — Activates the defense.
- disable — Deactivates the defense. This is the default.

Description

This command activates and deactivates the SYN ACK Flood DoS defense.

In this type of attack, an attacker, seeking to overwhelm a victim with TCP connection requests, sends a large number of TCP SYN packets with bogus source addresses to the victim. The victim responds with SYN ACK packets, but since the original source addresses are bogus, the victim node does not receive any replies. If the attacker sends enough requests in a short enough period, the victim may freeze operations once the requests exceed the capacity of its connections queue.

To defend against this form of attack, a switch port monitors the number of ingress TCP-SYN packets it receives. If a port receives more 60 TCP-SYN packets per second, the following occurs.

- The switch sends a trap to the management stations
- The switch blocks all traffic on the port for one minute.

This defense mechanism does not involve the switch's CPU. You can activate it on as many ports as you want without it impacting switch performance.

Example

The following command activates the defense on ports 18 to 20:

```
set dos synflood port=18-20 state=enable
```

SET DOS TEARDROP

Syntax

```
set dos teardrop port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port — Specifies the switch ports on which you want to enable or disable this DoS defense. You can select more than one port at a time.

state — Specifies the state of the DoS defense. The options are:

- enable — Activates the defense.
- disable — Deactivates the defense. This is the default.

mirroring — Specifies whether the examined traffic is copied to a mirror port. Options are:

- yes, on, true enabled — Traffic is mirrored. These values are equivalent.
- no, off, false disabled — Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command activates and deactivates the Teardrop DoS defense.

In this DoS attack, an attacker sends a packet in several fragments with a bogus offset value, used to reconstruct the packet, in one of the fragments to a victim. This results in the victim being unable to reassemble the packet, possibly causing it to freeze operations.

The defense mechanism for this type of attack has all ingress IP traffic received on a port sent to the switch's CPU. The CPU samples related, consecutive fragments, checking for fragments with invalid offset values. If one is found, the following occurs:

- The switch sends a trap to the management stations.
- The switch blocks all traffic on the port for one minute.

Because the CPU examines only a sampling of the ingress IP traffic on a port, there is no guarantee that the switch will catch or prevent all occurrences of this attack.

You can use the MIRRORING parameter to copy the offending traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to "SET SWITCH MIRROR" on page 194.

Caution

This defense is extremely CPU intensive and should be used with caution. Unrestricted use can cause a switch to halt operations if the CPU becomes overwhelmed with IP traffic. To prevent this, Allied Telesyn recommends that you activate this defense on only one port at a time and where ingress fragments comprise only a small percentage of the port's total traffic.

Example

The following command activates the defense on port 22:

```
set dos teardrop port=22 state=enable
```

SHOW DOS

Syntax 1

```
show dos [ipaddress] [subnet] [uplinkport]
```

Syntax 2

```
show dos defense port=port
```

Parameters

ipaddress	Displays the IP address of the LAN.
subnet	Displays the subnet mask.
uplinkport	Displays the uplink port for the Land defense.
defense	Displays the status of a specified defense for a particular port. Defense can be any of the following: synflood smurf land teardrop ipoption pingofdeath
port	Specifies the port whose DoS status you want to view. You can specify only one port.

Description

These commands display DoS status information. Syntax 1 displays the current settings for the IP address, subnet mask, and uplink port parameters. Syntax 2 displays DoS status information for a specific defense mechanism on a specific port.

Examples

The following command displays the IP address and subnet mask for the Land and SMURF defenses:

```
show dos ipaddress subnet
```

The following command displays the status of the SMURF defense on port 4:

```
show dos smurf port=4
```

Section III

IGMP Snooping, MLD Snooping, and RRP Snooping

The chapters in this section contain the commands for IGMP, MLD, and RRP snooping. The chapters include:

- Chapter 22, “IGMP Snooping Commands” on page 369
- Chapter 23, “MLD Snooping Commands” on page 379
- Chapter 24, “RRP Snooping Commands” on page 389

Chapter 22

IGMP Snooping Commands

This chapter contains the following commands:

- “DISABLE IGMPSNOOPING” on page 370
- “ENABLE IGMPSNOOPING” on page 371
- “SET IP IGMP” on page 372
- “SHOW IGMPSNOOPING” on page 375
- “SHOW IP IGMP” on page 376

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
For background information on this feature, refer to Chapter 19, “IGMP Snooping” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE IGMPSNOOPING

Syntax

```
disable igmpsnooping
```

Parameters

None.

Description

This command deactivates IGMP snooping on the switch.

Example

The following command deactivates IGMP snooping:

```
disable igmpsnooping
```

Equivalent Command

```
set ip igmp snoopingstatus=disabled
```

For information, refer to “SET IP IGMP” on page 372.

ENABLE IGMPSNOOPING

Syntax

```
enable igmpsnooping
```

Parameters

None.

Description

This command activates IGMP snooping on the switch.

Example

The following command activates IGMP snooping:

```
enable igmpsnooping
```

Equivalent Command

```
set ip igmp snoopingstatus=enabled
```

For information, refer to "SET IP IGMP" on page 372.

SET IP IGMP

Syntax

```
set ip igmp [snoopingstatus=enabled|disabled]
[hoststatus=singlehost|multihost] [timeout=value]
[numbermulticastgroups=value]
[routerport=port|all|none|auto]
```

Parameters

snoopingstatus — Activates and deactivates IGMP snooping on the switch. The options are:

- enabled — Activates IGMP snooping.
- disabled — Deactivates IGMP snooping. This is the default setting.

hoststatus — Specifies the IGMP host node topology. Options are:

- singlehost — Activates the Single-Host/Port setting, which is appropriate when there is only one host node connected to a port on the switch. This is the default setting.
- multihost — Activates the Multi-Host setting, which is appropriate if there is more than one host node connected to a switch port.

timeout — Specifies the time period in seconds at which the switch determines that a host node is inactive. An inactive host node is a node that has not sent an IGMP report during the specified time interval. The range is from 0 second to 86,400 seconds (24 hours). The default is 260 seconds. If you set the timeout to zero (0), the timer never times out, and the timeout interval is essentially disabled.

This parameter also controls the time interval used by the switch in determining whether a multicast router is still active. The switch makes the determination by watching

for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, the router is assumed to be no longer active on the port.

The actual timeout may be ten seconds less that the specified value. For example, a setting of 25 seconds can result in the switch classifying a host node or multicast router as inactive after just 15 seconds. A setting of 10 seconds or less can result in the immediate timeout of an inactive host node or router.

numbermulticastgroups — Specifies the maximum number of multicast addresses the switch learns. This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 to 255 addresses; the default is 64 addresses.

Note
The combined maximum number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

routerport — Specifies the port(s) on the switch connected to a multicast router. Options are:

port	Specifies the router port(s) manually.
all	Specifies all of the switch ports.
none	Sets the mode to manual without any router ports specified.
auto	Activates auto-detect, where the switch automatically determines the ports with multicast routers.

Description

This command configures the IGMP snooping parameters.

Examples

The following command activates IGMP snooping, sets the IGMP topology to Multi-Host, and sets the timeout value to 120 seconds:

```
set ip igmp snoopingstatus=enabled hoststatus=multihost
timeout=120
```

The following command changes the topology to Single-Host:

```
set ip igmp hoststatus=singlehost
```

The following command disables IGMP snooping:

```
set ip igmp snoopingstatus=disabled
```

Equivalent Commands

```
disable igmpsnooping
```

For information, refer to “DISABLE IGMPSNOOPING” on page 370.

```
enable igmpsnooping
```

For information, refer to “ENABLE IGMPSNOOPING” on page 371.

SHOW IGMPSNOOPING

Syntax

```
show igmpsnooping
```

Parameters

None.

Description

This command displays the IGMP parameters. Figure 38 illustrates the information that is displayed by this command.

```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Disabled
  Host Topology ...................... Single-Host/Port (Edge)
  Host/Router Timeout Interval ....... 260 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect
```

Figure 38. SHOW IGMPSNOOPING Command

For an explanation of these parameters, refer to "SET IP IGMP" on page 372.

Examples

The following command displays the current IGMP parameter settings:

```
show igmpsnooping
```

Equivalent Command

```
show ip igmp
```

For information, see "SHOW IP IGMP" on page 376.

SHOW IP IGMP

Syntax

```
show ip igmp [hostlist] [routerlist]
```

Parameters

hostlist	Displays a list of the multicast groups learned by the switch, as well as the ports on the switch that are connected to host nodes. This parameter displays information only when there are active host nodes.
routerlist	Displays the ports on the switch where multicast routers are detected. This parameter displays information only when there are active multicast routers.

Description

This command displays the IGMP parameters. Figure 39 illustrates the information that is displayed by this command without the optional parameters.

```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Disabled
  Host Topology ...................... Single-Host/Port (Edge)
  Host/Router Timeout Interval ....... 260 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect
```

Figure 39. SHOW IP IGMP Command

For an explanation of these parameters, refer to “SET IP IGMP” on page 372.

An example of the information displayed by the HOSTLIST parameter is shown in Figure 40.

```
Number of IGMP Multicast Groups: 1
   MulticastGroup ......... 01:00:5E:00:01:01
   VLAN ID ................ 1
   Port/TrunkID ........... 6
   HostIP ................. 172.16.10.51
   Version ................ v2
   Time ................... 21
```

Figure 40. SHOW IP IGMP Command with HOSTLIST Parameter

The HOSTLIST parameter displays the following information:

- Number of IGMP Multicast Groups - The number of IGMP multicast groups with active host nodes on the switch.
- Multicast Group - The multicast address of the group.
- VLAN - The VID of the VLAN where the port or trunk is an untagged member.
- Port/Trunk - The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number instead of the port number is displayed.
- HostIP - The IP address of the host node connected to the port.
- IGMP Ver. - The version of IGMP being used by the host.
- Exp. Time - The number of seconds remaining before the host is timed out if no further IGMP reports are received from it.

An example of the information displayed by the ROUTERLIST parameter is shown in Figure 41.

```
VLAN ............ 1
Port/Trunk ID ... 14
RouterIP ........ 172.16.01.1
```

Figure 41. SHOW IP IGMP Command with ROUTERLIST Parameter

The ROUTERLIST parameter displays the following information:

- VLAN - The VID of the VLAN in which the port is an untagged member.
- Port/Trunk ID - The port on the switch where the multicast router is connected. If the switch learned the router on a port trunk, the trunk ID number instead of the port number is displayed.
- Router IP - The IP address of the multicast router.

Examples

The following command displays the current IGMP parameter settings:

```
show ip igmp
```

The following command displays a list of active host nodes connected to the switch:

```
show ip igmp hostlist
```

The following command displays a list of active multicast routers:

```
show ip igmp routerlist
```

Equivalent Command

```
show igmpsnooping
```

This command does not display the router and host lists. For information, see “SHOW IGMPSNOOPING” on page 375.

Chapter 23

MLD Snooping Commands

This chapter contains the following commands:

- “DISABLE MLDSNOOPING” on page 380
- “ENABLE MLDSNOOPING” on page 381
- “SET IPV6 MLDSNOOPING” on page 382
- “SHOW MLDSNOOPING” on page 384
- “SHOW IPV6 MLDSNOOPING” on page 386

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
For background information on this feature, refer to Chapter 20, “MLD Snooping” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE MLDSNOOPING

Syntax

```
disable mldsnooping
```

Parameters

None.

Description

This command deactivates MLD snooping on the switch.

Example

The following command deactivates MLD snooping:

```
disable mldsnooping
```

Equivalent Command

```
set ipv6 mldsnooping snoopingstatus=disabled
```

For information, refer to “SET IPV6 MLDSNOOPING” on page 382.

ENABLE MLDSNOOPING

Syntax

```
enable mldsnooping
```

Parameters

None.

Description

This command activates MLD snooping on the switch.

Example

The following command activates MLD snooping:

```
enable mldsnooping
```

Equivalent Command

```
set ipv6 mldsnooping snoopingstatus=enabled
```

For information, refer to "SET IPV6 MLDSNOOPING" on page 382.

SET IPV6 MLDSNOOPING

Syntax

```
set ipv6 mldsnooping [snoopingstatus=enabled|disabled]
[hoststatus=singlehost|multihost] [timeout=value]
[numbermulticastgroups=value]
[routerport=port|all|none|auto]
```

Parameters

snoopingstatus — Activates and deactivates MLD snooping on the switch. The options are:

- **enabled** — Activates MLD snooping.
- **disabled** — Deactivates MLD snooping. This is the default setting.

hoststatus — Specifies the MLD host node topology. Options are:

- **singlehost** — Activates the Single-Host/Port setting, which is appropriate when there is only one host node connected to a port on the switch. This is the default setting.
- **multihost** — Activates the Multi-Host setting, which is appropriate if there is more than one host node connected to a switch port.

timeout — Specifies the time period, in seconds, used by the switch in determining inactive host nodes. An inactive host node is a node that has not sent an MLD report during the specified time interval. The range is 1 to 86,400 seconds (24 hours); the default is 260 seconds.

numbermulticastgroups — Specifies the maximum number of multicast addresses the switch learns. This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or

static MAC addresses. The range is 1 to 255 addresses; the default is 64 addresses.

Note
The combined number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

routerport	Specifies the port(s) on the switch connected to a multicast router. Options are:
port	Specifies the router port(s) manually.
all	Specifies all of the switch ports.
none	Sets the mode to manual without any router ports specified.
auto	Activates auto-detect, where the switch automatically determines the ports with multicast routers.

Description

This command configures the MLD snooping parameters.

Example

The following command activates MLD snooping, sets the MLD topology to Multi-Host, and sets the timeout value to 120 seconds:

```
set ipv6 mldsnooping snoopingstatus=enabled
hoststatus=multihost timeout=120
```

The following command changes the topology to Single-Host:

```
set ipv6 mldsnooping hoststatus=singlehost
```

The following command disables MLD snooping:

```
set ipv6 mldsnooping snoopingstatus=disabled
```

Equivalent Commands

```
disable mldsnooping
```

For information, see "DISABLE MLDSNOOPING" on page 380.

```
enable mldsnooping
```

For information, see "ENABLE MLDSNOOPING" on page 381.

SHOW MLDSNOOPING

Syntax

```
show mldsnooping
```

Parameters

None.

Description

This command displays the following MLD parameters:

- MLD snooping status
- Multicast host topology
- Host/router timeout interval
- Maximum multicast groups
- Host and router lists

To set the MLD parameters, refer to “SET IPV6 MLDSNOOPING” on page 382.

This command displays the information in Figure 42.

```
MLD Snooping Configuration:
 MLD Snooping Status ................ Enabled
 Host Topology ...................... Single-Host/Port (Edge)
 Host/Router Timeout Interval ....... 260 seconds
 Maximum MLD Multicast Groups ....... 64
 Router Port(s) ..................... Auto Detect

Host List:
Number of MLD Multicast Groups: 1
                  VLAN   Port/                                                  Exp.
MulticastGroup    ID     TrunkID    HostIP                                      Time
-------------------------------------------------------------------------------------
33:33:00:00:00:ab 1      6          fe80:0000:0000:0000:0208:74ff:feff:bf08     21

Router List:
VLAN       Port/Trunk ID       RouterIP
-------------------------------------------------------------------------------------
1          14                  fe80:0000:0000:0000:0200:cdff:fe12:bf08
```

Figure 42. SHOW MLDSNOOPING Command

The parameters in the MLD Snooping Configuration section are explained “SET IPV6 MLDSNOOPING” on page 382.

The Host List section displays the following information:

- Multicast Group - The multicast address of the group.
- VLAN - The VID of the VLAN where the port is an untagged member.
- Port/TrunkID - The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number, not the port number, is displayed.
- HostIP - The IP address of the host node connected to the port.
- Exp. Time - The number of seconds remaining before the host is timed out if no further MLD reports are received from it.

The Router List section displays this information:

- VLAN - The VID of the VLAN in which the port is an untagged member.
- Port/Trunk ID - The port on the switch where the multicast router is connected. If the switch learned the router on a port trunk, the trunk ID number, not the port number, is displayed.
- Router IP - The IP address of the multicast router.

Example

The following command displays the current MLD parameter settings, along with the host and router lists:

```
show mldsnooping
```

Equivalent Command

```
show ipv6 mldsnooping hostlist routerlist
```

For information, see "SHOW IPV6 MLDSNOOPING" on page 386.

SHOW IPV6 MLDSNOOPING

Syntax

```
show ipv6 mldsnooping [hostlist] [routerlist]
```

Parameters

hostlist	Displays a list of the multicast groups learned by the switch, as well as the ports on the switch that are connected to host nodes. This parameter displays information only when there are active host nodes.
routerlist	Displays the ports on the switch where multicast routers are detected. This parameter displays information only when there are active multicast routers.

Description

This command displays the following MLD parameters:

- MLD snooping status
- Multicast host topology
- Host/router timeout interval
- Maximum multicast groups
- Multicast router port(s)
- Host and router lists

For instructions on how to set the MLD parameters, refer to “SET IPV6 MLDSNOOPING” on page 382.

This command without optional parameters displays the information in Figure 43.

```
MLD Snooping Configuration:
 MLD Snooping Status ............... Enabled
 Host Topology ..................... Single-Host/Port (Edge)
 Host/Router Timeout Interval ....... 260 seconds
 Maximum MLD Multicast Groups ....... 64
 Router Port(s) ..................... Auto Detect
```

Figure 43. SHOW IPV6 MLDSNOOPING Command

Refer to "SET IPV6 MLDSNOOPING" on page 382 for an explanation of the parameters.

The HOSTLIST option displays the information in Figure 44.

```
Host List:
Number of MLD Multicast Groups: 1
                        VLAN    Port/                                                   Exp.
MulticastGroup          ID      TrunkID    HostIP                                       Time
-------------------------------------------------------------------------------------------
33:33:00:00:00:ab       1       6          fe80:0000:0000:0000:0208:74ff:feff:bf08      21
```

Figure 44. SHOW IPV6 MLDSNOOPING Command with HOSTLIST Option

The information is described here:

- Multicast Group - The multicast address of the group.
- VLAN - The VID of the VLAN where the port is an untagged member.
- Port/TrunkID - The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number, not the port number, is displayed.
- HostIP - The IP address of the host node connected to the port.
- Exp. Time - The number of seconds remaining before the host is timed out if no further MLD reports are received from it.

The ROUTERLIST option displays the information in Figure 45.

```
Router List:
VLAN    Port/Trunk ID   RouterIP
-----------------------------------------------------------
1       14              fe80:0000:0000:0000:0200:cdff:fe12:bf08
```

Figure 45. SHOW IPV6 MLDSNOOPING Command with ROUTERLIST Option

The information displayed by the option is described here:

- VLAN - The VID of the VLAN in which the port is an untagged member.
- Port/Trunk ID - The port on the switch where the multicast router is connected. If the switch learned the router on a port trunk, the trunk ID number, not the port number, is displayed.
- Router IP - The IP address of the multicast router.

Examples

The following command displays the current MLD parameter settings:

```
show ipv6 mldsnooping
```

The following command displays a list of active host nodes connected to the switch:

```
show ipv6 mldsnooping hostlist
```

The following command displays a list of active multicast routers:

```
show ipv6 mldsnooping routerlist
```

Equivalent Command

```
show mldsnooping
```

For information, see “SHOW MLDSNOOPING” on page 384.

Chapter 24

RRP Snooping Commands

This chapter contains the following commands:

- “DISABLE RRPSNOOPING” on page 390
- “ENABLE RRPSNOOPING” on page 391
- “SHOW RRPSNOOPING” on page 392

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 21, “RRP Snooping” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE RRPSNOOPING

Syntax

```
disable rrpsnooping
```

Parameters

None.

Description

This command disables RRP snooping. This is the default setting.

Example

The following command disables RRP snooping:

```
disable rrpsnooping
```

ENABLE RRPSNOOPING

Syntax

```
enable rrpsnooping
```

Parameters

None.

Description

This command enables RRP snooping.

Example

The following command activates RRP snooping on the switch:

```
enable rrpsnooping
```

SHOW RRPSNOOPING

Syntax

```
show rrpsnooping
```

Parameter

None.

Description

This command displays the status of RRP snooping, enabled or disabled.

Example

The following command displays the status of RRP snooping:

```
show rrpsnooping
```

Section IV
SNMPv3

The chapter in this section contains the commands for SNMPv3. The chapter is:

- Chapter 25, “SNMPv3 Commands” on page 395

Chapter 25

SNMPv3 Commands

This chapter contains the following commands:

- “ADD SNMPV3 USER” on page 397
- “CLEAR SNMPV3 ACCESS” on page 399
- “CLEAR SNMPV3 COMMUNITY” on page 401
- “CLEAR SNMPV3 NOTIFY” on page 402
- “CLEAR SNMPV3 TARGETADDR” on page 403
- “CLEAR SNMPV3 VIEW” on page 404
- “CREATE SNMPV3 ACCESS” on page 405
- “CREATE SNMPV3 COMMUNITY” on page 408
- “CREATE SNMPV3 GROUP” on page 410
- “CREATE SNMPV3 NOTIFY” on page 412
- “CREATE SNMPV3 TARGETADDR” on page 414
- “CREATE SNMPV3 TARGETPARAMS” on page 416
- “CREATE SNMPV3 VIEW” on page 418
- “DELETE SNMPV3 USER” on page 420
- “DESTROY SNMPv3 ACCESS” on page 421
- “DESTROY SNMPv3 COMMUNITY” on page 423
- “DESTROY SNMPv3 GROUP” on page 424
- “DESTROY SNMPv3 NOTIFY” on page 425
- “DESTROY SNMPv3 TARGETADDR” on page 426
- “DESTROY SNMPv3 TARGETPARMS” on page 427
- “DESTROY SNMPV3 VIEW” on page 428
- “PURGE SNMPV3 ACCESS” on page 429
- “PURGE SNMPV3 COMMUNITY” on page 430
- “PURGE SNMPV3 NOTIFY” on page 431
- “PURGE SNMPV3 TARGETADDR” on page 432
- “PURGE SNMPV3 VIEW” on page 433
- “SET SNMPV3 ACCESS” on page 434
- “SET SNMPV3 COMMUNITY” on page 436
- “SET SNMPV3 GROUP” on page 438

- ❒ “SET SNMPV3 NOTIFY” on page 440
- ❒ “SET SNMPV3 TARGETADDR” on page 442
- ❒ “SET SNMPV3 TARGETPARAMS” on page 444
- ❒ “SET SNMPV3 USER” on page 446
- ❒ “SET SNMPV3 VIEW” on page 448
- ❒ “SHOW SNMPV3 ACCESS” on page 450
- ❒ “SHOW SNMPV3 COMMUNITY” on page 451
- ❒ “SHOW SNMPv3 GROUP” on page 452
- ❒ “SHOW SNMPV3 NOTIFY” on page 453
- ❒ “SHOW SNMPV3 TARGETADDR” on page 454
- ❒ “SHOW SNMPV3 TARGETPARAMS” on page 455
- ❒ “SHOW SNMPV3 USER” on page 456
- ❒ “SHOW SNMPV3 VIEW” on page 457

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 22, “SNMPv3” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD SNMPV3 USER

Syntax

```
add snmpv3 user=user [authentication=md5|sha]
authpassword=password privpassword=password
[storagetype=volatile|nonvolatile]
```

Parameters

user — Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

authentication — Specifies the authentication protocol that is used to authenticate this user with an SNMP entity (manager or NMS). If you do not specify an authentication protocol, this parameter is automatically set to None. The options are:

- md5 — The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.
- sha — The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

  Note: You must specify the authentication protocol before you specify the authentication password.

authpassword — Specifies a password for the authentication protocol, up to 32 alphanumeric characters. If you specify an authentication protocol, then you must configure an authentication protocol password.

privpassword — Specifies a password for the 3DES privacy, or encryption protocol, up to 32 alphanumeric characters. This is an optional parameter.

Note: If you specify a privacy password, the privacy protocol is set to DES. You must also specify an authentication protocol and password.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table

	entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 User Table entry.

Examples

The following command creates an SNMPv3 user with the name “steven142” with an authentication protocol of MD5, an authentication password of “99doublesecret12”, a privacy password of “encrypt178” and a storage type of nonvolatile.

```
add snmpv3 user=steven142 authentication=md5
authpassword=99doublesecret12 privpassword=encrypt178
storagetype=nonvolatile
```

The following command creates an SNMPv3 user with the name “77hoa” an authentication protocol of SHA, an authentication password of “youvegottobekidding88” and a storage type of nonvolatile.

```
add snmpv3 user=77hoa authentication=sha
authpassword=youvegottobekidding88 storagetype=nonvolatile
```

CLEAR SNMPV3 ACCESS

Syntax

```
clear snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] readview writeview notifyview
```

Parameters

access — Specifies the name of the security group, up to 32 alphanumeric characters.

securitymodel — Specifies the security model. The options are:

- v1 — Associates the Security Name, or User Name, with the SNMPv1 protocol.
- v2c — Associates the Security Name, or User Name, with the SNMPv2c protocol.
- v3 — Associates the Security Name, or User Name, with the SNMPv3 protocol.

securitylevel — Specifies the security level. The options are:

- noauthentication — This option provides no authentication protocol and no privacy protocol.
- authentication — This option provides an authentication protocol, but no privacy protocol.
- privacy — This option provides an authentication protocol and the privacy protocol.

readview — Specifies a Read View Name that allows the users assigned to this security group to view the information specified by the View Table entry. This is an optional parameter.

writeview — Specifies a Write View Name that allows the users assigned to this security group to write, or modify, the information in the specified View Table. This is an optional parameter.

notifyview	Specifies a Notify View Name that allows the users assigned to this security group to send traps permitted in the specified View. This is an optional parameter.

Description

This command clears the specified fields in an SNMPv3 Access Table entry.

Examples

The following command clears the readview parameter in a security group called “Engineering” which has a security model of the SNMPv3 protocol and a security level of privacy.

```
clear snmpv3 access=Engineering securitymodel=v3
securitylevel=privacy readview
```

The following command clears the values in the readview, writeview, and notifyview parameters in a security group called “SystemTest.” This group has a security model of the SNMPv3 protocol and a security level of authentication.

```
clear snmpv3 access=SystemTest securitymodel=v3
securitylevel=authentication readview writeview notifyview
```

CLEAR SNMPV3 COMMUNITY

Syntax

```
clear snmpv3 community index=index transporttag
```

Parameters

index	Specifies the name of an existing SNMPv3 Community Table entry, up to 32 alphanumeric characters.
transporttag	Specifies the transport tag, up to 32 alphanumeric characters.

Description

This command clears the transporttag parameter in an SNMPv3 Community Table entry.

Examples

The following command clears the value of the transporttag parameter in the SNMPv3 Community Table entry with an index of 1005:

```
clear snmpv3 community index=1005 transporttag
```

The following command clears the value of the transporttag parameter in the SNMPv3 Community Table entry with an index of 421:

```
clear snmpv3 community index=421 transporttag
```

CLEAR SNMPV3 NOTIFY

Syntax

```
clear snmpv3 notify=notify tag
```

Parameters

notify	Specifies the name of an SNMPv3 Notify Table entry, up to 32 alphanumeric characters.
tag	Specifies the notify tag name, up to 32 alphanumeric characters.

Description

This command clears the value of the tag parameter in an SNMPv3 Notify Table entry.

Examples

The following command deletes the value of the tag parameter in an SNMPv3 Notify Table entry called “hwengtrap:”

```
clear snmpv3 notify=hwengtraptag tag
```

The following command deletes the value of the tag parameter in an SNMPv3 Notify Table entry called “hwenginformtag:”

```
clear snmpv3 notify=hwenginform tag
```

CLEAR SNMPV3 TARGETADDR

Syntax

```
clear snmpv3 targetaddr=targetaddr taglist
```

Parameters

targetaddr	Specifies the name of the SNMPv3 Target Address Table entry, up to 32 alphanumeric characters.
taglist	Specifies a tag or list of tags, up to 256 alphanumeric characters.

Description

This command clears the value of the taglist parameter in an SNMPv3 Target Address Table entry.

Examples

The following command deletes the value of the taglist parameter from the SNMPv3 Target Address Table entry called "snmphost79:"

```
clear snmpv3 targetaddr=snmphost44 taglist
```

The following command deletes the value of the taglist parameter from the SNMPv3 Target Address Table entry called "snmphost79:"

```
clear snmpv3 targetaddr=snmphost79 taglist
```

CLEAR SNMPV3 VIEW

Syntax

```
clear snmpv3 view=view [subtree=OID|text] mask
```

Parameters

view	Specifies the name of the SNMPv3 view, up to 32 alphanumeric characters.
subtree	Specifies the view of the MIB Tree. Options are: OID A numeric value in hexadecimal format. text Text name of the view.
mask	Specifies the subtree mask, in hexadecimal format.

Description

This command clears the value of the mask parameter in an SNMPv3 View Table entry.

Examples

The following command clears the value of the subtree mask from the SNMPv3 view of 1.3.6.1.2.1.1:

```
clear snmpv3 view=1.3.6.1.2.1.1 mask
```

The following command clears the value of subtree mask from the SNMPv3 view called private. The subtree has a value of 1.3.6.1.4 (private MIBs).

```
clear snmpv3 view=private subtree=1.3.6.1.4 mask
```

CREATE SNMPV3 ACCESS

Syntax

```
create snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] readview=readview writeview=writeview
notifyview=notifyview [storagetype=volatile|nonvolatile]
```

Parameters

access — Specifies the name of the security group, up to 32 alphanumeric characters.

securitymodel — Specifies the security model. The options are:

- v1 — Associates the Security Name, or User Name, with the SNMPv1 protocol.
- v2c — Associates the Security Name, or User Name, with the SNMPv2c protocol.
- v3 — Associates the Security Name, or User Name, with the SNMPv3 protocol.

securitylevel — Specifies the security level. The options are:

- noauthentication — This option provides no authentication protocol and no privacy protocol.
- authentication — This option provides an authentication protocol, but no privacy protocol.

privacy — This option provides an authentication protocol and the privacy protocol.

readview — Specifies a Read View Name that allows the users assigned to this Group Name to view the information specified by the View Table entry. This is an optional parameter. If you do not assign a value to this parameter, then the readview parameter defaults to none.

writeview — Specifies a Write View Name that allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This is an optional parameter. If you do not assign a value to this parameter, then the writeview parameter defaults to none.

notifyview — Specifies a Notify View Name that allows the users assigned to this Group Name to send traps permitted in the specified View. This is an optional parameter. If you do not assign a value to this parameter, then the notifyview parameter defaults to none.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Access Table entry.

Examples

The following command creates a security group called “testengineering” with a security model of SNMPv3 and a security level of privacy. The security group has a read view named “internet,” a write view named private, and a notify view named “internet.” The storage type is nonvolatile storage.

```
create snmpv3 access=testengineering securitymodel=v3
securitylevel=privacy readview=internet writeview=private
notifyview=internet storage=nonvolatile
```

The following command creates a security group called “swengineering” with a security model of SNMPv3 and a security level of authentication. In addition, the security group has a read view named “internet,” a write view named experimental, and a notify view named “mgmt” (management). The storage type group is nonvolatile storage.

```
create snmpv3 access=swengineering securitymodel=v3
securitylevel=authentication readview=internet
writeview=experimental notifyview=mgmt storage=nonvolatile
```

The following command creates a security group called “hwengineering” with a security model of SNMPv3 and a security level of noauthentication. In addition, the security group has a read view named “internet.”

```
create snmpv3 access=hwengineering securitymodel=v3
securitylevel=authentication readview=internet
```

Note
In the above example, the storage type has not been specified. As a result, the storage type for the hwengineering security group is volatile storage.

CREATE SNMPV3 COMMUNITY

Syntax

```
create snmpv3 community index=index
communityname=communityname securityname=securityname
transporttag=transporttag
[storagetype=volatile|nonvolatile]
```

Parameters

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.
communityname	Specifies a password for this community entry, up to 32 alphanumeric characters.
securityname	Specifies the name of an SNMPv1 and SNMPv2 user, up to 32 alphanumeric characters.
transporttag	Specifies the transport tag, up to 32 alphanumeric characters. This is an optional parameter.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Community Table entry.

Examples

The following command creates an SNMP community with an index of 1213 and a community name of “sunnyvale145.” The user is “chitra34” and the transport tag is “testengtag.” The storage type for this community is nonvolatile storage.

```
create snmpv3 community index=1213
communityname=sunnyvale145 securityname=chitra34
transporttag=testengtag storagetype=nonvolatile
```

The following command creates an SNMP community with an index of 95 and a community name of "12sacramento49." The user is "regina" and the transport tag "trainingtag." The storage type for this community is nonvolatile storage.

```
create snmpv3 community index=95
communityname=12sacramento49 securityname=regina
transporttag=trainingtag storagetype=nonvolatile
```

CREATE SNMPV3 GROUP

Syntax

```
create snmpv3 group username=username
[securitymodel=v1|v2c|v3] groupname=groupname
[storagetype=volatile|nonvolatile]
```

Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are: v1 Associates the Security Name, or User Name, with the SNMPv1 protocol. v2c Associates the Security Name, or User Name, with the SNMPv2c protocol. v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.
groupname	Specifies a group name configured in the SNMPv3 Access Table with the access parameter. See “CREATE SNMPV3 ACCESS” on page 405.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: volatile Does not allow you to save the table entry to the configuration file on the switch. This is the default. nonvolatile Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 SecurityToGroup Table entry.

Examples

The following command creates the SNMPv3 SecurityToGroup Table entry for a user named Nancy. The security model is set to the SNMPv3 protocol. The group name, or security group, for this user is the “admin” group. The storage type is set to nonvolatile storage.

```
create snmpv3 group username=Nancy securitymodel=v3
groupname=admin storagetype=nonvolatile
```

The following command creates the SNMPv3 SecurityToGroup Table entry for a user named princess. The security model is set to the SNMPv3 protocol. The group name, or security group, for this user is the "training" group. The storage type is set to nonvolatile storage.

```
create snmpv3 group username=princess securitymodel=v3
groupname=training storagetype=nonvolatile
```

CREATE SNMPV3 NOTIFY

Syntax

```
create snmpv3 notify=notify tag=tag [type=trap|inform]
[storagetype=volatile|nonvolatile]
```

Parameters

notify	Specifies the name of an SNMPv3 Notify Table entry, up to 32 alphanumeric characters.
tag	Specifies the notify tag name, up to 32 alphanumeric characters. This is an optional parameter.
type	Specifies the message type. This is an optional parameter. The options are:
trap	Trap messages are sent, with no response expected from another entity (NMS or manager). This is the default.
inform	Inform messages are sent, with a response expected from another entity (NMS or manager).
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:
volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Notify Table entry.

Examples

The following command creates the SNMPv3 Notify Table entry called “testengtrap1” and the notify tag is “testengtag1.” The message type is defined as a trap message and the storage type for this entry is nonvolatile storage.

```
create snmpv3 notify=testengtrap1 tag=testengtag1 type=trap
storagetype=nonvolatile
```

The following command creates the SNMPv3 Notify Table entry called "testenginform5" and the notify tag is "testenginformtag5." The message type is defined as an inform message and the storage type for this entry is nonvolatile storage.

```
create snmpv3 notify=testenginform5 tag=testenginformtag5
type=inform storagetype=nonvolatile
```

CREATE SNMPV3 TARGETADDR

Syntax

```
create snmpv3 targetaddr=targetaddr params=params
ipaddress=ipaddress udpport=udpport timeout=timeout
retries=retries taglist=taglist
[storagetype=volatile|nonvolatile]
```

Parameters

targetaddr	Specifies the name of the SNMP manager, or host, that manages the SNMP activity on the switch, up to 32 alphanumeric characters.
params	Specifies the target parameters name, up to 32 alphanumeric characters.
ipaddress	Specifies the IP address of the host.
udpport	Specifies the UDP port in the range of 0 to 65535. The default UDP port is 162. This is an optional parameter.
timeout	Specifies the timeout value in milliseconds. The range is 0 to 2,147,483,647 milliseconds, and the default is 1500 milliseconds. This is an optional parameter.
retries	Specifies the number of times the switch resends an inform message. The default is 3. This is an optional parameter.
taglist	Specifies a tag or list of tags, up to 256 alphanumeric characters. Use a space to separate entries. This is an optional parameter.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Target Address Table entry.

Examples

In the following command, the name of the Target Address Table entry is "snmphost1." In addition, the params parameter is assigned to "snmpv3manager" and the IP address is 198.1.1.1. The tag list consists of "swengtag," "hwengtag," and "testengtag." The storage type for this table entry is nonvolatile storage.

```
create snmpv3 targetaddr=snmphost1 params=snmpv3manager
ipaddress=198.1.1.1 taglist=swengtag hwengtag testengtag
storagetype=nonvolatile
```

In the following command, the name of the Target Address Table entry is snmphost99. The params parameter is "snmpmanager7" and the IP address is 198.1.2.2. The tag list is "trainingtag." The storage type for this table entry is nonvolatile storage.

```
create snmpv3 targetaddr=snmphost99 params=snmpmanager7
ipaddress=198.1.2.2 taglist=trainingtag
storagetype=nonvolatile
```

CREATE SNMPV3 TARGETPARAMS

Syntax

```
create snmpv3 targetparams=targetparams username=username
[securitymodel=v1|v2c|v3] [messageprocessing=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] [storagetype=volatile|nonvolatile]
```

Parameters

targetparams	Specifies the name of the SNMPv3 Target Parameters Table entry, up to 32 alphanumeric characters.
username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are: v1 Associates the User Name, or Security Name, with the SNMPv1 protocol. v2c Associates the User Name, or Security Name, with the SNMPv2c protocol. v3 Associates the User Name, or Security Name, with the SNMPv3 protocol.
messageprocessing	Specifies the SNMP protocol that is used to process, or send messages. Configure this parameter only if you have selected the SNMPv1 or SNMPv2c protocols as the security model. If you have selected the SNMPv3 protocol as the security model, message processing is automatically set to the SNMPv3 protocol. The options are: v1 Messages are processed with the SNMPv1 protocol. v2c Messages are processed with the SNMPv2c protocol. v3 Messages are processed with the SNMPv3 protocol.

securitylevel	Specifies the security level. The options are:	
	noauthentication	This option provides no authentication protocol and no privacy protocol.
	authentication	This option provides an authentication protocol, but no privacy protocol.
	privacy	This option provides an authentication protocol and the privacy protocol.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Target Parameters Table entry.

Examples

In the following command, the Target Parameters Table entry is called "snmpv3mgr13" and user name is "user444." The security model is set to the SNMPv3 protocol. In addition, the security level is set to privacy and the storage type is nonvolatile.

```
create snmpv3 targetparams=snmpv3mgr13 username=user444
securitymodel=v3 securitylevel=privacy
storagetype=nonvolatile
```

In the following command, the Target Parameters Table entry is called "snmpmanager" and the user name is "pat365." The security model is set to SNMPv3 protocol. In addition, the security level is set to authentication and the storage type is nonvolatile.

```
create snmpv3 targetparams=snmpmanager username=pat365
securitymodel=v3 securitylevel=authentication
storagetype=nonvolatile
```

CREATE SNMPV3 VIEW

Syntax

```
create snmpv3 view=view [subtree=OID|text] mask=mask
[type=included|excluded]
[storagetype=volatile|nonvolatile]
```

Parameters

view	Specifies the name of the view, up to 32 alphanumeric characters.	
subtree	Specifies the view of the MIB Tree. The options are:	
	OID	A numeric value in hexadecimal format.
	text	Text name of the view.
mask	Specifies the subtree mask, in hexadecimal format.	
type	Specifies the view type. This is an optional parameter. The options are:	
	included	Permits a user to view the specified subtree. This is the default.
	excluded	Does not permit a user to view the specified subtree.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 View Table entry.

Examples

The following command creates an SNMPv3 View Table entry called “internet1” with a subtree value of the Internet MIBs and a view type of included. The storage type for this table entry is nonvolatile storage.

```
create snmpv3 view=internet1 subtree=internet type=included
storagetype=nonvolatile
```

The following command creates an SNMPv3 View Table entry called "tcp1" with a subtree value of the TCP/IP MIBs and a view type of excluded. The storage type for this table entry is nonvolatile storage.

```
create snmpv3 view=tcp1 subtree=tcp type=excluded
storagetype=nonvolatile
```

DELETE SNMPV3 USER

Syntax

```
delete snmpv3 user=user
```

Parameters

user	Specifies the name of an SNMPv3 user to delete from the switch.

Description

This command deletes an SNMPv3 User Table entry. After you delete an SNMPv3 user from the switch, you cannot recover it.

Examples

The following command deletes the user named “wilson890.”

```
delete snmpv3 user=wilson890
```

The following command deletes the user named “75murthy75.”

```
delete snmpv3 user=75murthy75
```

DESTROY SNMPv3 ACCESS

Syntax

```
destroy snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy]
```

Parameter

access	Specifies an SNMPv3 Access Table entry.
securitymodel	Specifies the security model of the user name specified above. The options are: v1 Associates the Security Name, or User Name, with the SNMPv1 protocol. v2c Associates the Security Name, or User Name, with the SNMPv2c protocol. v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.
securitylevel	Specifies the security level. The options are: noauthentication This option provides no authentication protocol and no privacy protocol. authentication This option provides an authentication protocol, but no privacy protocol. privacy This option provides an authentication protocol and the privacy protocol.

Description

This command deletes an SNMPv3 Access Table entry. After you delete an SNMPv3 Access Table entry, you cannot recover it.

Examples

The following command deletes the SNMPv3 Access Table entry called "swengineering" with a security model of the SNMPv3 protocol and a security level of authentication.

```
destroy snmpv3 access=swengineering securitymodel=v3
securitylevel=authentication
```

The following command deletes the SNMPv3 Access Table entry called “testengineering” with a security model of the SNMPv3 protocol and a security level of privacy.

```
destroy snmpv3 access=testengineering securitymodel=v3
securitylevel=privacy
```

DESTROY SNMPv3 COMMUNITY

Syntax

```
destroy snmpv3 community index=index
```

Parameter

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.

Description

This command deletes an SNMPv3 Community Table entry. After you delete an SNMPv3 Community Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 Community Table entry with an index of 1001.

```
destroy snmpv3 community index=1001
```

The following command deletes an SNMPv3 Community Table entry with an index of 5.

```
destroy snmpv3 community index=5
```

DESTROY SNMPv3 GROUP

Syntax

```
destroy snmpv3 group username=username
[securitymodel=v1|v2c|v3]
```

Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are:
	v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.
	v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.
	v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

Description

This command deletes an SNMPv3 SecurityToGroup Table entry. After you delete an SNMPv3 SecurityToGroup Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 User Table entry for a user called Dave with an security model of the SNMPv3 protocol:

```
destroy snmpv3 group username=Dave securitymodel=v3
```

The following command deletes an SNMPv3 User Table entry for a user called May with an security model of the SNMPv3 protocol:

```
destroy snmpv3 group username=May securitymodel=v3
```

DESTROY SNMPv3 NOTIFY

Syntax

```
destroy snmpv3 notify=notify
```

Parameter

notify	Specifies an SNMPv3 Notify Table entry.

Description

This command deletes an SNMPv3 Notify Table entry. After you delete an SNMPv3 Notify Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 Notify Table entry called "systemtestnotifytrap."

```
destroy snmpv3 notify=systemtestnotifytrap
```

The following command deletes an SNMPv3 Notify Table entry called "engineeringinform1."

```
destroy snmpv3 notify=engineeringinform1
```

DESTROY SNMPv3 TARGETADDR

Syntax

```
destroy snmpv3 targetaddr=target
```

Parameter

targetaddr	Specifies an SNMPv3 Target Address table entry.

Description

This command deletes an SNMPv3 Target Address Table entry. After you delete an SNMPv3 Target Address Table entry, you cannot recover it.

Example

The following command deletes an SNMPv3 Address Table entry called "snmpmanager."

```
destroy snmpv3 targetaddr=snmpmanager
```

DESTROY SNMPv3 TARGETPARMS

Syntax

```
destroy snmpv3 targetparams=targetparams
```

Parameter

targetparams	Specifies an SNMPv3 Target Parameters table entry.

Description

This command deletes an SNMPv3 Target Parameters Table entry. After you delete an SNMPv3 Target Parameters Table entry, you cannot recover it.

Examples

The following command deletes the SNMPv3 Target Parameters Table entry called "targetparameter1."

```
destroy snmpv3 targetparams=targetparameter1
```

The following command deletes the SNMPv3 Target Parameters Table entry called "snmpmanager."

```
destroy snmpv3 targetparams=snmpmanager
```

DESTROY SNMPV3 VIEW

Syntax

```
destroy snmpv3 view=view [subtree=OID|text]
```

Parameters

view	Specifies the name of the view, up to 32 alphanumeric characters.
subtree	Specifies the view subtree view. The options are: OID A numeric value in hexadecimal format. text Text name of the view.

Description

This command deletes an SNMPv3 View Table entry. After you delete an SNMPv3 View Table entry, you cannot recover it.

Examples

The following command deletes the SNMPv3 View Table entry named “experimental. “ The subtree value of this table entry is experimental.

```
destroy snmpv3 view=experimental subtree=experimental
```

The following command deletes the SNMPv3 View Table entry named “directory.” The subtree value of this table entry is 1.3.6.1.3.

```
destroy snmpv3 view=directory subtree=1.3.6.1.3
```

PURGE SNMPV3 ACCESS

Syntax

```
purge snmpv3 access
```

Parameters

None

Description

This command resets the SNMPv3 Access Table to its default value by removing all the access table entries. To remove a single entry, use "DESTROY SNMPv3 ACCESS" on page 421.

Example

The following example removes all the SNMPv3 Access Table entries:

```
purge snmpv3 access
```

PURGE SNMPV3 COMMUNITY

Syntax

```
purge snmpv3 community
```

Parameters

None

Description

This command resets the SNMPv3 Community Table to its default value by removing all the community table entries. To remove a single entry, use “DESTROY SNMPv3 COMMUNITY” on page 423.

Example

The following example removes all the SNMPv3 Community Table entries:

```
purge snmpv3 community
```

PURGE SNMPV3 NOTIFY

Syntax

```
purge snmpv3 notify
```

Parameters

None

Description

This command resets the SNMPv3 Notify Table to its default value by removing all the notify table entries. To remove a single entry, use "DESTROY SNMPv3 NOTIFY" on page 425.

Example

The following example removes all the entries from the SNMPv3 Notify Table:

```
purge snmpv3 notify
```

PURGE SNMPV3 TARGETADDR

Syntax

```
purge snmpv3 targetaddr
```

Parameters

None

Description

This command resets the SNMPv3 Target Address Table to its default values by removing all the target address table entries. To remove a single entry, use “DESTROY SNMPv3 TARGETADDR” on page 426.

Example

The following example removes all the entries from the SNMPv3 Target Address Table:

```
purge snmpv3 targetaddr
```

PURGE SNMPV3 VIEW

Syntax

```
purge snmpv3 view
```

Parameters

None

Description

This command resets the SNMPv3 View Table to its default values by removing all the view table entries. To remove a single entry, use "DESTROY SNMPV3 VIEW" on page 428.

Example

The following example removes all the entries from the SNMPv3 View Table:

```
purge snmpv3 view
```

SET SNMPV3 ACCESS

Syntax

```
set snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] readview=readview writeview=writeview
notifyview=notifyview [storagetype=volatile|nonvolatile]
```

Parameters

access	Specifies the name of the group, up to 32 alphanumeric characters.
securitymodel	Specifies the security model. Options are: v1 Associates the Security Name, or User Name, with the SNMPv1 protocol. v2c Associates the Security Name, or User Name, with the SNMPv2c protocol. v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.
securitylevel	Specifies the security level. The options are: noauthentication This option provides no authentication protocol and no privacy protocol. authentication This option provides an authentication protocol, but no privacy protocol. privacy This option provides an authentication protocol and the privacy protocol.
readview	Specifies a Read View Name that allows the users assigned to this Group Name to view the information specified by the View Table entry.
writeview	Specifies a Write View Name that allows the users assigned to this Security Group to write, or modify, the information in the specified View Table.
notifyview	Specifies a Notify View Name that allows the users assigned to this Group Name to send traps permitted in the specified View.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Access Table entry.

Examples

The following command modifies the group called engineering. The new read view is the Internet MIBs and the storage type is volatile storage.

```
set snmpv3 access=engineering securitymodel=v3
securitylevel=authentication readview=internet
storagetype=volatile
```

The following command modifies the group called training. The read view, write view, and notify view are set to the Internet MIBs. The storage type is nonvolatile storage.

```
set snmpv3 access=training securitymodel=v3
securitylevel=privacy readview=internet writeview=internet
notifyview=internet storagetype=nonvolatile
```

SET SNMPV3 COMMUNITY

Syntax

```
set snmpv3 community index=index communityname=communityname
securityname=securityname transporttag=transporttag
[storagetype=volatile|nonvolatile]
```

Parameters

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.
communityname	Specifies a password of this community, up to 32 alphanumeric characters.
securityname	Specifies the name of an SNMPv1 and SNMPv2 user, up to 32 alphanumeric characters.
transporttag	Specifies the transport tag, up to 32 alphanumeric characters.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Community Table entry.

Examples

The following command modifies the community table entry with an index of 1001. The community has a password of “secretpassword98” and a security name of “user451.” The transport tag is set to “sampletag4” and the storage type is set to nonvolatile storage.

```
set snmpv3 community index=1001
communityname=secretpassword98 securityname=user451
transporttag=sampletag4 storagetype=nonvolatile
```

The following command modifies the community table entry with an index of 52. The community has a password of “oldmiss71” and a security name of “jjhuser234.” The transport tag is set to “testtag40.”

```
set snmpv3 community index=52 communityname=oldmiss71
securityname=jjhuser234 transporttag=testtag40
```

SET SNMPV3 GROUP

Syntax

```
set snmpv3 group username=username [securitymodel=v1|v2c|v3]
groupname=groupname [storagetype=volatile|nonvolatile]
```

Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are:
	v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.
	v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.
	v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.
groupname	Specifies a group name configured in the SNMPv3 Access Table.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:
volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 SecurityToGroup Table entry.

Examples

The following command modifies the SecurityToGroup Table entry with a user name of “nancy28.” The security model is the SNMPv3 protocol. and the group name is set to engineering.

```
set snmpv3 group username=nancy28 securitymodel=v3
groupname=engineering
```

The following command modifies the SecurityToGroup Table entry with a user name of "nelvid." The security model is the SNMPv3 protocol and the group name "systemtest."

```
set snmpv3 group username=nelvid securitymodel=v3
groupname=systemtest
```

SET SNMPV3 NOTIFY

Syntax

```
set snmpv3 notify=notify tag=tag [type=trap|inform]
[storagetype=volatile|nonvolatile]
```

Parameters

notify	Specifies the name associated with the trap message, up to 32 alphanumeric characters.	
tag	Specifies the notify tag name, up to 32 alphanumeric characters.	
type	Specifies the message type. Options are:	
	trap	Trap messages are sent, with no response expected from the host.
	inform	Inform messages are sent, with a response expected from the host.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Notify Table entry.

Examples

The following command modifies an SNMPv3 Notify Table entry called “systemtesttrap2.” The notify tag is “systemtesttag2” and the message type is a trap message.

```
set snmpv3 notify=systemtesttrap2 tag=systemtesttag2
type=trap
```

The following command modifies an SNMPv3 Notify Table entry called "systemtestinform5." The notify tag is "systemtestinform5tag" and the message type is an inform message.

```
set snmpv3 notify=systemtestinform5 tag=systemtestinform5tag
type=inform
```

SET SNMPV3 TARGETADDR

Syntax

```
set snmpv3 targetaddr=targetaddr params=params
ipaddress=ipaddress udpport=udpport timeout=timeout
retries=retries taglist=taglist
[storagetype=volatile|nonvolatile]
```

Parameters

targetaddr	Specifies the name of the SNMP entity (NMS or manager) that manages the SNMP activity on the switch, up to 32 alphanumeric characters.
params	Specifies the target parameters name, up to 32 alphanumeric characters. This is an optional parameter.
ipaddress	Specifies the IP address of the host. This is an optional parameter.
udpport	Specifies the UDP port in the range of 0 to 65535. The default UDP port is 162. This is an optional parameter.
timeout	Specifies the timeout value in milliseconds. The range is 0 to 2,147,483,647 milliseconds, and the default is 1500 milliseconds. This is an optional parameter.
retries	Specifies the number of times the switch retries to send an inform message. The default is 3. This is an optional parameter.
taglist	Specifies a tag or list of tags, up to 256 alphanumeric characters. Use a space to separate entries. This is an optional parameter.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:
	volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
	nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Target Address Table entry.

Examples

The following command modifies the Target Address Table entry with a value of "snmphost." The params parameter is set to "targetparameter7" and the IP address is 198.1.1.1. The taglist is set to "systemtesttraptag" and "systemtestinformtag."

```
set snmpv3 targetaddr=snmphost params=targetparameter7
ipaddress=198.1.1.1 taglist=systemtesttraptag
systemtestinformtag
```

The following command modifies the Target Address Table entry with a value of "host." The params parameter is set to "targetparameter22" and the IP address is 198.1.1.198. The taglist is set to "engineeringtraptag" and "engineeringinformtag."

```
set snmpv3 targetaddr=host params=targetparameter22
ipaddress=198.1.1.198 taglist=engineeringtraptag
engineeringinformtag
```

SET SNMPV3 TARGETPARAMS

Syntax

```
set snmpv3 targetparams=targetparams username=username
[securitymodel=v1|v2c|v3] [messageprocessing=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] [storagetype=volatile|nonvolatile]
```

Parameters

targetparams — Specifies the target parameters name, up to 32 alphanumeric characters.

username — Specifies the user name.

securitymodel — Specifies the security model of the above user name. The options are:

- v1 — Associates the Security Name, or User Name, with the SNMPv1 protocol.
- v2c — Associates the Security Name, or User Name, with the SNMPv2c protocol.
- v3 — Associates the Security Name, or User Name, with the SNMPv3 protocol.

messageprocessing — Specifies the SNMP protocol that is used to process, or send messages. Configure this parameter only if you have selected the SNMPv1 or SNMPv2c protocols as the security model. If you have selected the SNMPv3 protocol as the security model, message processing is automatically set to the SNMPv3 protocol. The options are:

- v1 — Messages are processed with the SNMPv1 protocol.
- v2c — Messages are processed with the SNMPv2c protocol.
- v3 — Messages are processed with the SNMPv3 protocol.

securitylevel — Specifies the security level. The options are:

- noauthentication — This option provides no authentication protocol and no privacy protocol.

	authentication	This option provides an authentication protocol, but no privacy protocol.
	privacy	This option provides an authentication protocol and the privacy protocol.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are:	
	volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
	nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies a Target Parameters Table entry.

Examples

The following command modifies the Target Parameters Table entry called "host23." The user name is "user7990" and the security model is the SNMPv3 protocol. The security level is set to the privacy level.

```
set snmpv3 targetparams=host23 username=loan1
securitymodel=v3 securitylevel=privacy
```

The following command modifies the Target Parameters Table entry called "manager9". The user name is "loan1" and the security model is the SNMPv3 protocol. The security level is set to the authentication protocol.

```
set snmpv3 targetparams=manager9 username=loan1
securitymodel=v3 securitylevel=authentication
```

SET SNMPV3 USER

Syntax

```
set snmpv3 user=user [authentication=md5|sha]
authpassword=password privpassword=password
[storagetype=volatile|nonvolatile]
```

Parameters

user — Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

authentication — Specifies the authentication protocol that is used to authenticate this user with an SNMPv3 entity (or NMS). The default is no authentication. The options are:

- md5 — The MD5 authentication protocol. Users are authenticated with the MD5 authentication protocol after a message is received.
- sha — The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

authpassword — Specifies a password for the authentication protocol, up to 32 alphanumeric characters.

privpassword — Specifies a password for the 3DES privacy, or encryption protocol, up to 32 alphanumeric characters. Configuring a privacy protocol password, turns on the DES privacy protocol.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 User Table entry.

Examples

The following command modifies a User Table entry called "atiuser104". The authentication protocol is set to the MD5 protocol and the authentication password is "atlanta45denver." The DES privacy protocol is on and the privacy password is "denvertoatlanta3."

```
set snmpv3 user=atiuser104 authentication=md5
authpassword=atlanta45denver privpassword=denvertoatlanta3
```

The following command modifies a User Table entry called "atiuser104." The authentication protocol is set to the MD5 protocol and the authentication password is "nycbostonwash56." The privacy protocol is on and the privacy password is "bostontoamherst7." The storage type is set to nonvolatile storage.

```
set snmpv3 user=atiuser104 authentication=md5
authpassword=nycbostonwash56 privpassword=bostontoamherst7
storagetype=nonvolatile
```

SET SNMPV3 VIEW

Syntax

```
set snmpv3 view=view [subtree=OID|text] mask=mask
[type=included|excluded]
[storagetype=volatile|nonvolatile]
```

Parameters

view	Specifies the name of the view, up to 32 alphanumeric characters.
subtree	Specifies the view subtree view. Options are: OID A numeric value in hexadecimal format. text Text name of the view.
mask	Specifies the subtree mask, in hexadecimal format.
type	Specifies the view type. Options are: included Permits the user assign to this View Name to see the specified subtree. excluded Does not permit the user assigned to this View Name to see the specified subtree.
storagetype	Specifies the storage type of this table entry. This is an optional parameter. The options are: volatile Does not allow you to save the table entry to the configuration file on the switch. This is the default. nonvolatile Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 View Table entry.

Examples

The following command modifies the view called “internet1.” The subtree is set to the Internet MIBs and the view type is included.

```
set snmpv3 view=internet1 subtree=internet type=included
```

The following command modifies the view called system. The subtree is set to 1.3.6.1.2.1 (System MIBs) and the view type is excluded.

```
set snmpv3 view=system subtree=1.3.6.1.2.1 type=excluded
```

SHOW SNMPV3 ACCESS

Syntax

```
show snmpv3 access=access
```

Parameter

access	Specifies an SNMPv3 Access Table entry.

Description

This command displays the SNMPv3 Access Table. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 Access Table entry called “production.”

```
show snmpv3 access=production
```

The following command displays all of the SNMPv3 Access Table entries:

```
show snmpv3 access
```

SHOW SNMPV3 COMMUNITY

Syntax

```
show snmpv3 community index=index
```

Parameter

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.

Description

This command displays the SNMPv3 Community Table. You can display one or all of the SNMPv3 Community Table entries.

Examples

The following command displays the Community Table entry with an index of 246:

```
show snmpv3 community index=246
```

The following command displays all of the Community Table entries:

```
show snmpv3 community
```

SHOW SNMPv3 GROUP

Syntax

```
show snmpv3 group username=username
[securitymodel=v1|v2c|v3]
```

Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are:
	v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.
	v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.
	v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

Description

This command displays SNMPv3 SecurityToGroup Table entries. You can display one or all of the table entries.

Example

The following command displays the SNMPv3 SecurityToGroup Table entry for a user named Dave who is assigned a security model of the SNMPv3 protocol.

```
show snmpv3 group username=Dave securitymodel=v3
```

The following command displays all of the SNMPv3 SecurityToGroup Table entries:

```
show snmpv3 group
```

SHOW SNMPV3 NOTIFY

Syntax

```
show snmpv3 notify=notify
```

Parameter

notify	Specifies an SNMPv3 Notify Table entry.

Description

This command displays SNMPv3 Notify Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 Notify Table entry called "testengtrap1":

```
show snmpv3 notify=testengtrap1
```

The following command displays all of the SNMPv3 Notify Table entries:

```
show snmpv3 notify
```

SHOW SNMPV3 TARGETADDR

Syntax

```
show snmpv3 targetaddr=targetaddr
```

Parameter

targetaddr	Specifies an SNMPv3 Target Address Table entry.

Description

This command displays SNMPv3 Target Address Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 Target Address Table entry called “snmpv3host55”:

```
show snmpv3 targetaddr=snmpv3host55
```

The following command displays all of the SNMPv3 Target Address Table entries:

```
show snmpv3 targetaddr
```

SHOW SNMPV3 TARGETPARAMS

Syntax

```
show snmpv3 targetparams=targetparams
```

Parameter

targetparams Specifies an SNMPv3 Target Parameters Table entry.

Description

This command displays SNMPv3 Target Parameters Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 Target Parameters Table entry called "snmpv3manager95":

```
show snmpv3 targetparams=snmpv3manager95
```

The following command displays all of the SNMPv3 Target Parameters Table entries:

```
show snmpv3 targetparams
```

SHOW SNMPV3 USER

Syntax

```
show snmpv3 user=user
```

Parameters

userSpecifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

Description

This command displays SNMPv3 User Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 User Table entry for a user name of Robert:

```
show snmpv3 user=Robert
```

The following command displays all of the SNMPv3 User Table entries:

```
show snmpv3 user
```

SHOW SNMPV3 VIEW

Syntax

```
show snmpv3 view=view [subtree=OID|text]
```

Parameter

view	Specifies an SNMPv3 View Table entry.
subtree	Specifies the view subtree view. Options are:
	OID A numeric value in hexadecimal format.
	text Text name of the view.

Description

This command displays the SNMPv3 View Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 View Table entry called "snmpv3manager95":

```
show snmpv3 targetparams=snmpv3manager95
```

The following command displays all the SNMPv3 View Table entries:

```
show snmpv3 targetparams
```

Section V

Spanning Tree Protocols

The chapters in this section contain the commands for the spanning tree protocols. The chapters include:

- Chapter 26, “Spanning Tree Protocol Commands” on page 461
- Chapter 27, “Rapid Spanning Tree Protocols Commands” on page 475
- Chapter 28, “Multiple Spanning Tree Protocol Commands” on page 489

Chapter 26

Spanning Tree Protocol Commands

This chapter contains the following commands:

- ❒ “ACTIVATE STP” on page 462
- ❒ “DISABLE STP” on page 463
- ❒ “ENABLE STP” on page 464
- ❒ “PURGE STP” on page 465
- ❒ “SET STP” on page 466
- ❒ “SET STP PORT” on page 469
- ❒ “SET SWITCH MULTICASTMODE” on page 471
- ❒ “SHOW STP” on page 473

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 23, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ACTIVATE STP

Syntax

```
activate stp
```

Parameters

None.

Description

Use this command to designate STP as the active spanning tree on the switch. You cannot enable STP or configure its parameters until you have designated it as the active spanning tree with this command.

Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on the switch at a time.

Example

The following command designates STP as the active spanning tree:

```
activate stp
```

DISABLE STP

Syntax

```
disable stp
```

Parameters

None.

Description

This command disables the Spanning Tree Protocol on the switch. The default setting for STP is disabled. To view the current status of STP, refer to "SHOW STP" on page 473.

Example

The following command disables STP:

```
disable stp
```

ENABLE STP

Syntax

```
enable stp
```

Parameters

None.

Description

This command enables the Spanning Tree Protocol on the switch. The default setting for STP is disabled. To view the current status of STP, refer to “SHOW STP” on page 473.

> **Note**
> You cannot enable STP until after you have activated it with “ACTIVATE STP” on page 462.

Example

The following command enables STP on the switch:

```
enable stp
```

PURGE STP

Syntax

```
purge stp
```

Parameters

None.

Description

This command returns all STP bridge and port parameters to the default settings. STP must be disabled in order for you to use this command. To disable STP, see "DISABLE STP" on page 463.

Example

The following command resets the STP parameter settings to their default values:

```
purge stp
```

Equivalent Command

```
set stp default
```

For information, see "SET STP" on page 466.

SET STP

Syntax

```
set stp [default] [priority=priority] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
```

Parameters

default — Disables STP and returns all bridge and port STP settings to the default values. This parameter cannot be used with any other command parameter and can only be used when STP is disabled. (This parameter performs the same function as the PURGE STP command.)

priority — Specifies the priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge.

The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 12. You specify the increment that represents the desired bridge priority value. The default value is 32,768 (increment 8).

Table 12. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

hellotime — Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

forwarddelay — Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, all links may not have had time to adapt to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

maxage — Specifies the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. The range is 6 to 40 seconds. The default is 20 seconds.

Note
The value for the maxage parameter must be greater than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

Description

This command sets the following STP parameters:

- Bridge priority
- Hello time
- Forwarding delay
- Maximum age time

This command can also disable STP and return the STP parameters to their default settings.

Note
You can use this command only if STP is designated as the active spanning tree protocol on the switch. See "ACTIVATE STP" on page 462.

Examples

The following command sets the switch's bridge priority value to 45,056 (increment 11):

```
set stp priority=11
```

The following command sets the hello time to 7 seconds and the forwarding delay to 25 seconds:

```
set stp hellotime=7 forwarddelay=25
```

The following command returns all STP parameters on the switch to the default values:

```
set stp default
```

Equivalent Command

```
purge stp
```

For information, see "PURGE STP" on page 465.

SET STP PORT

Syntax

```
set stp port=port [pathcost|portcost=auto|portcost]
[portpriority=portpriority]
```

Parameters

port — Specifies the port you want to configure. You can configure more than one port at a time. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

pathcost ***or*** portcost — Specifies the port's cost. The parameters are equivalent. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost to the root bridge for that LAN. This parameter can take the range of 1 to 65,535, or AUTO. The default setting is AUTO, for Automatic Update, which automatically sets port cost according to the speed of the port. Table 13 lists the STP port costs with Auto-Detect.

Table 13. STP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

Table 14 lists the STP port costs with Auto-Detect when a port is part of a port trunk.

Table 14. Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	4
100 Mbps	4
1000 Mbps	1

portpriority — Specifies the port's priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16, for a total of 16 increments as

shown in Table 15. You specify the increment of the desired value. The default is 128 (increment 8).

Table 15. Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Description

This command configures the following STP parameter settings for a switch port:

- Port cost
- Port priority

Examples

The following command sets the port cost to 15 and the port priority to 192 (increment 12) for port 6:

```
set stp port=6 portcost=15 portpriority=12
```

The following command sets the port cost to auto-detect on ports 7 to 10:

```
set stp port=7-10 portcost=auto
```

SET SWITCH MULTICASTMODE

Syntax

```
set switch multicastmode=[a|b|c|d]
```

Parameter

multicast mode — Specifies the multicast mode. The options are:

- a — Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all ports.
- b — Forwards ingress spanning tree BPDU and 802.1x EAPOL packets across all VLANs and ports.
- c — Forwards ingress BPDU and EAPOL packets only among the untagged ports of the VLAN where the ingress port is a member.
- d — Forwards ingress BPDU and EAP packets on both tagged and untagged ports of the VLAN where the ingress port is a member.

Description

This command controls the behavior of the switch when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets when these features are disabled on the switch. Note the following when setting this parameter:

- You can only set this parameter from this command. You cannot configure it from the menus or web browser interface.
- The mode is set at the switch level. You cannot configure it on a per-port basis.
- A switch can have only one mode active at a time.
- The mode setting applies to spanning tree protocol BPDUs when STP, RSTP, and MSTP are disabled on the switch.
- The mode setting applies to 802.1x port-based access control EAPOL packets when 802.1x is disabled.
- There are four possible states: A, B, C, and D:

A - Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all ports. The switch behaves as follows:

- If STP, RSTP, and MSTP are disabled, all ingress BPDUs are discarded.

- If 802.1x port-based access control is disabled, all ingress EAPOL packets are discarded.

B - Forwards ingress spanning tree BPDU and 802.1x EAPOL packets across all VLANs and ports. This is the default setting. The switch behaves as follows:

- If STP, RSTP, and MSTP are disabled, ingress BPDUs are flooded on all ports.
- If STP, RSTP, MSTP, and 802.1x are disabled on the switch, BPDUs and EAPOL packets are flooded on all ports.
- If the switch is running STP or RSTP and 802.1x is disabled, EAPOL packets are flooded on all ports, except ports in the blocking state.
- If the switch is running MSTP and 802.1x is disabled, EAPOL packets are flooded on all ports, including ports in the blocking state.

C - Forwards ingress BPDU and EAPOL packets only on untagged ports of the VLAN where the ingress port is a member. Packets are not forwarded from tagged ports. The VLAN is identified by the PVID assigned to the ingress port.

D - Forwards ingress BPDU and EAP packets from both tagged and untagged ports of the VLAN where the ingress port is a member. The VLAN is identified by the PVID assigned to the ingress port.

Example

The following command sets the switch's mode to A to discard all ingress BPDUs and 802.1 EAPOL packets:

```
set switch multicastmode=a
```

SHOW STP

Syntax

```
show stp [port=port]
```

Parameter

port — Specifies the port whose STP parameters you want to view. You can view more than one port at a time.You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

Description

This command displays the current values for the STP parameters. An example of the display is shown in Figure 46.

```
Status ..................... Enabled
Bridge Priority ............ 32768 (In multiples of 4096: 8)
Bridge Hello Time .......... 2/2 (Configured/Actual)
Bridge Forwarding Delay ..... 15/15 (Configured/Actual)
Bridge Max Age ............. 20/20 (Configured/Actual)
Bridge Identifier .......... 32768/00:21:46:A7:B4:11
Root Bridge ................ 32768/00:21:46:A7:B4:11
Root Path Cost ............. 0
```

Figure 46. SHOW STP Command

The bridge priority, bridge hello time, and bridge max age parameters display two values when STP is enabled on the switch (for example, Bridge Forwarding Delay .. 15/15). The first number is the configured value on the switch for the parameter and the second is the value the switch obtained from the root bridge and is actually using for the parameter. The switch displays only the configured values when spanning tree is not activated on the switch.

The Status parameter displays whether STP is enabled or disabled on the switch.

For definitions of the bridge priority, hello time, forwarding delay, and max age parameters, refer to "SET STP" on page 466.

The bridge Identifier parameter consists of the switch's bridge priority value and MAC address, separated by a slash (/). To change the switch's priority value, refer to "SET STP" on page 466. The MAC address of the switch cannot be changed.the MAC address of the switch.

The root bridge parameter specifies the bridge identifier of the root bridge of the spanning tree domain. The identifier consists of the bridge priority value and MAC address of the root switch, separated by a slash (/). This parameter only appears when STP is activated on the switch.

The root path cost parameter displays the path cost from the switch to the root bridge of the spanning tree domain. If the switch is the root bridge, the path cost is 0. This parameter only appears when STP is activated on the switch.

The PORT parameter allows you to view the STP parameter settings for the switch ports: An example of the display is shown in Figure 47.

```
Port  State           Cost     Priority
-----------------------------------------------
1     Forwarding      4        128
2     Forwarding      4        128
3     Forwarding      4        128
4     Forwarding      4        128
5     Forwarding      4        128
6     Forwarding      4        128
7     Forwarding      4        128
8     Forwarding      4        128
9     Forwarding      4        128
10    Forwarding      4        128
11    Forwarding      4        128
```

Figure 47. SHOW STP PORT Command

Port is the port number.

State is the current state of a port. The possible states are Listening, Learning, Forwarding, or Blocking when spanning tree is enabled on the switch. When spanning tree is not enabled on the switch or if a port is not being used, its state will be disabled.

Cost is the port cost of the port.

Priority is the port's priority value. The number is used as a tie breaker when two or more ports have equal costs to the root bridge.

Examples

The following command displays the switch's STP settings:

```
show stp
```

The following command displays the STP settings for ports 1 to 4:

```
show stp port=1-4
```

Chapter 27

Rapid Spanning Tree Protocols Commands

This chapter contains the following commands:

- ❒ “ACTIVATE RSTP” on page 476
- ❒ “DISABLE RSTP” on page 477
- ❒ “ENABLE RSTP” on page 478
- ❒ “PURGE RSTP” on page 479
- ❒ “SET RSTP” on page 480
- ❒ “SET RSTP PORT” on page 483
- ❒ “SHOW RSTP” on page 486

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 23, “Spanning Tree and Rapid Spanning Tree Protocols” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ACTIVATE RSTP

Syntax

```
activate rstp
```

Parameters

None.

Description

Use this command to designate RSTP as the active spanning tree on the switch. After you have selected RSTP, you can enable or disable it using the ENABLE RSTP and DISABLE RSTP commands. RSTP is active on a switch only after you have designated it as the active spanning tree with this command and enabled it with the ENABLE RSTP command.

Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on the switch at a time.

Example

The following command designates RSTP as the active spanning tree:

```
activate rstp
```

DISABLE RSTP

Syntax

```
disable rstp
```

Parameters

None.

Description

This command disables the Rapid Spanning Tree Protocol on the switch. To view the current status of RSTP, use "SHOW RSTP" on page 486.

Example

The following command disables RSTP:

```
disable rstp
```

ENABLE RSTP

Syntax

```
enable rstp
```

Parameters

None.

Description

This command enables the Rapid Spanning Tree Protocol on the switch. The default setting for RSTP is disabled. To view the current status of RSTP, use “SHOW RSTP” on page 486.

You cannot enable RSTP until you have activated it with the ACTIVATE RSTP command.

Example

The following command enables RSTP:

```
enable rstp
```

PURGE RSTP

Syntax

```
purge rstp
```

Parameters

None.

Description

This command returns all RSTP bridge and port parameters to the default settings. RSTP must be disabled before you can use this command. To disable RSTP, refer to "DISABLE RSTP" on page 477.

Example

The following command resets RSTP:

```
purge rstp
```

Equivalent Command

```
set rstp default
```

For information, refer to "SET RSTP" on page 480.

SET RSTP

Syntax

```
set rstp [default] [priority=priority] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
[rstptype|forceversion=stpcompatible|
forcestpcompatible|normalrstp]
```

Parameters

default — Returns all bridge and port RSTP settings to the default values. This parameter cannot be used with any other command parameter and only when RSTP is disabled. (This parameter performs the same function as the PURGE RSTP command.)

priority — Specifies the priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 16. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 16. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

hellotime	Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.
forwarddelay	Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds. This parameter effects only those ports operating in the STP compatible mode.
maxage	Specifies the length of time, in seconds, after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

Note
The value for the maxage parameter must be greater than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

rstptype ***or*** forceversion	Sets the RSTP mode. The parameters are equivalent. The options are:	
	stpcompatible ***or*** forcestpcompatible	The bridge uses the RSTP parameter settings, but transmits only STP BPDU packets from the ports. These options are equivalent.
	normalrspt	The bridge uses RSTP. It transmits RSTP BPDU packets, except on ports connected to bridges running STP. This is the default setting.

Description

This command configures the following RSTP parameter settings.

- Bridge priority
- Hello time

- ❒ Forwarding delay
- ❒ Maximum age time
- ❒ Port priority
- ❒ Force version of STP or normal RSTP

This command can also return the RSTP parameters to their default settings.

Note
You can use this command only if RSTP is the active spanning tree protocol on the switch. See “ACTIVATE RSTP” on page 476.

Examples

The following command sets the bridge priority to 20480 (increment 5), the hello time to 5 seconds, and the forwarding delay to 20 seconds:

```
set rstp priority=5 hellotime=5 forwarddelay=20
```

The following command uses the FORCEVERSION parameter to configure the bridge to use the RSTP parameters but to transmit only STP BPDU packets:

```
set rstp forceversion=stpcompatible
```

The following command returns all RSTP parameter settings to their default values:

```
set rstp default
```

Equivalent Command

```
purge rstp
```

For information, see “PURGE RSTP” on page 479.

SET RSTP PORT

Syntax

```
set rstp port=port [pathcost|portcost=cost|auto]
[portpriority=portpriority]
[edgeport=yes|no|on|off|true|false]
[ptp|pointtopoint=yes|no|on|off|true|false|autoupdate]
[migrationcheck=yes|no|on|off|true|false]
```

Parameters

port — Specifies the port you want to configure. You can specify more than one port at a time. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

pathcost ***or*** portcost — Specifies the port's cost. The parameters are equivalent. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The options are:

- cost — A number for the port cost. The range is 1to 200,000,000.
- auto — Automatically sets the port cost according to the speed of the port. This is the default. Table 17 lists the port cost with auto-detect.

Table 17. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 18 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 18. RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000

Table 18. RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
100 Mbps	20,000
1000 Mbps	2,000

portpriority — Specifies the port's priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16, for a total of 16 increments, as shown in Table 19. You specify the increment that corresponds to the desired value. The default is 128, which is increment 8.

Table 19. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

edgeport — Defines whether the port is functioning as an edge port. An edge port is connected to a device operating at half-duplex mode and is not connected to any device running STP or RSTP. The options are:

- yes, on, true — The port is an edge port. The options are equivalent. This is the default.
- no, off, false — The port is not an edge port. The options are equivalent.

ptp ***or*** pointtopoint — Defines whether the port is functioning as a point-to-point port. The parameters are equivalent. This type of port is connected to a device operating at full-duplex mode. The options are:

	yes, on, true	The port is an point-to-point port. The options are equivalent.
	no, off, false	The port is not an point-to-point port. The parameters are equivalent. are equivalent.
	autoupdate	The port's status is determined automatically. This is the default.
migrationcheck	Enables and disables migration check. The purpose of this feature is to change from the RSTP mode to the STP mode if STP BDPU packets are received on the selected port. When you enable this option, the bridge will send out RSTP BPDU packets from the selected port until STP BPDU packets are received. The port will remain in the RSTP mode until it receives an STP BPDU packet. The options are:	
	yes, on, true	Enable migration check. The options are equivalent.
	no, off, false	Disable migration check. The options are equivalent.

Description

This command sets a port's RSTP settings.

Examples

The following command sets the port cost to 1,000,000 and port priority to 224 (increment 14) on port 4:

```
set rstp port=4 portcost=1000000 portpriority=14
```

The following command changes ports 6 to 8 so they are not considered edge ports:

```
set rstp port=6-8 edgeport=no
```

SHOW RSTP

Syntax

```
show rstp [portconfig=port|portstate=port]
```

Parameters

portconfig	Displays the RSTP port settings. You can specify more than one port at a time.
portstate	Displays the RSTP port status. You can specify more than one port at a time.

Description

You can use this command to display the RSTP parameter settings. An example of the display is shown in Figure 48.

```
Status ..................... Enabled
Force Version ............... NormalRSTP
Bridge Priority ............. 32768 (In multiples of 4096: 8)
Bridge Hello Time ........... 2/2 (Configured/Actual)
Bridge Forward Delay ........ 15/15 (Configured/Actual)
Bridge Max Age .............. 20/20 (Configured/Actual)
Bridge Identifier ........... 32768/00:21:46:A7:B4:11
Root Bridge Identifier ...... 32768/00:21:46:A7:B4:11
Root Path Cost .............. 0
```

Figure 48. Example of the SHOW RSTP Command

The bridge priority, bridge hello time, and bridge max age parameters will have two values if RSTP is enabled on the switch (for example, Bridge Forwarding .. 15/15). The first number is the configured value on the switch for the parameter and the second is the value the switch obtained from the root bridge and is currently using for the parameter. The switch displays only the configured values for these parameters if spanning tree is not enabled on the switch.

The Status parameter displays whether STP is enabled or disabled on the switch.

For definitions of the force version, bridge priority, hello time, forward delay, and max age parameters, refer to “SET RSTP” on page 480.

The bridge Identifier parameter consists of the switch’s bridge priority value and MAC address, separated by a slash (/). To change the switch’s priority value, refer to “SET RSTP” on page 480. The MAC address of the switch cannot be changed.

The root bridge identifier parameter displays the bridge priority value and MAC address of the root switch of the spanning tree domain. The values are separated by a slash (/). This parameter only appears when RSTP is activated on the switch.

The root path cost parameter displays the path cost from the switch to the root bridge of the spanning tree domain. If the switch is the root bridge, the path cost is 0. This parameter only appears when RSTP is activated on the switch.

The PORTCONFIG parameter displays the current RSTP parameter settings for the ports. An example is shown in Figure 49.

```
Port    | Edge-Port |Point-to-Point |    Cost      |  Priority
-----------------------------------------------------------------

1          Yes         Auto Update     Auto Update     128
2          Yes         Auto Update     Auto Update     128
3          Yes         Auto Update     Auto Update     128
4          Yes         Auto Update     Auto Update     128
5          Yes         Auto Update     Auto Update     128
6          Yes         Auto Update     Auto Update     128
7          Yes         Auto Update     Auto Update     128
8          Yes         Auto Update     Auto Update     128
10         Yes         Auto Update     Auto Update     128
11         Yes         Auto Update     Auto Update     128
```

Figure 49. Example of the SHOW RSTP PORTCONFIG Command

For definitions of these parameters, refer to "SET RSTP PORT" on page 483 or the *AT-S63 Management Software Menus Interface User's Guide*.

The PORTSTATE parameter displays the current operating settings and status of the ports. An example is shown in Figure 50.

```
Port     State          Role         Edge   P2P   Version   Port-Cost
-----------------------------------------------------------------
1        Disabled       ----------------------------------
2        Forwarding     Designated   No     Yes   RSTP      200000
3        Forwarding     Designated   No     Yes   RSTP      200000
4        Forwarding     Designated   No     Yes   RSTP      200000
5        Forwarding     Designated   No     Yes   RSTP      200000
6        Forwarding     Designated   No     Yes   RSTP      200000
7        Forwarding     Designated   No     Yes   RSTP      200000
8        Forwarding     Designated   No     Yes   RSTP      200000
9        Forwarding     Designated   No     Yes   RSTP      200000
10       Forwarding     Designated   No     Yes   RSTP      200000
11       Forwarding     Designated   No     Yes   RSTP      200000
```

Figure 50. Example of the SHOW RSTP PORTSTATE Command

The information displayed by the command is as follows:

- Port — The port number.
- State — The RSTP state of the port. The possible states for a port connected to another device running RSTP are Discarding and Forwarding.

  The possible states for a port connected to a device running STP are Listening, Learning, Forwarding, and Blocking.

  The possible states for a port not being used or where spanning tree is not activated is Disabled.
- Role — The RSTP role of the port. Possible roles are:

  Root - The port is connected to the root switch, directly or through other switches, with the least path cost.

  Alternate - The port offers an alternate path to the root switch.

  Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

  Designated - The port has the least cost path to the root switch.
- P2P — Whether or not the port is functioning as a point-to-point port. The possible settings are Yes and No.
- Version — Whether the port is operating in RSTP mode or STP-compatible mode.
- Port Cost — The current operating cost of the port.

Examples

The following command displays the bridge's RSTP settings:

```
show rstp
```

The following command displays the RSTP port settings for ports 1 to 4:

```
show rstp portconfig=1-4
```

The following command displays RSTP port status for port 15:

```
show rstp portstate=15
```

Chapter 28

Multiple Spanning Tree Protocol Commands

This chapter contains the following commands:

- “ACTIVATE MSTP” on page 490
- “ADD MSTP” on page 491
- “CREATE MSTP” on page 492
- “DELETE MSTP” on page 493
- “DESTROY MSTP MSTIID” on page 494
- “DISABLE MSTP” on page 495
- “ENABLE MSTP” on page 496
- “PURGE MSTP” on page 497
- “SET MSTP” on page 498
- “SET MSTP CIST” on page 501
- “SET MSTP MSTI” on page 502
- “SET MSTP MSTIVLANASSOC” on page 504
- “SET MSTP PORT” on page 505
- “SHOW MSTP” on page 509

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 24, “Multiple Spanning Tree Protocol” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ACTIVATE MSTP

Syntax

```
activate mstp
```

Parameters

None.

Description

This command designates MSTP as the active spanning tree on the switch. You cannot enable MSTP or configure its parameters until after you have designated it as the active spanning tree with this command.

Only one spanning tree protocol can be active on the switch at a time.

Example

The following command designates MSTP as the active spanning tree:

```
activate mstp
```

ADD MSTP

Syntax

```
add mstp mstiid=mstiid mstivlanassoc=vids
```

Parameters

mstiid	Specifies the ID of the multiple spanning tree instance (MSTI) to which you want to associate VLANs. You can specify only one MSTI ID at a time. The range is 1 to 15.
mstivlanassoc	Specifies the VID of the VLAN you want to associate with the MSTI ID. You can specify more than one VID at a time (for example, 2,5,44).

Description

This command associates VLANs to a MSTI.

The MSTIID parameter specifies the MSTI ID. The MSTI must already exist on the switch. To create a spanning tree instance, see "CREATE MSTP" on page 492.

The MSTIVLANASSOC parameter specifies the VIDs of the VLANs you want to associate with the MSTI. The VLANs must already exist on the switch. Any VLANs already associated with the MSTI are retained. If you want to add VLANs to a MSTI while removing those already associated to it, see "SET MSTP MSTIVLANASSOC" on page 504.

Examples

The following command associates the VLAN with the VID 4 to MSTI ID 8:

```
add mstp mstiid=8 mstivlanassoc=4
```

The following command associates the VLANs with the VIDs 24 and 44 to MSTI ID 11:

```
add mstp mstiid=11 mstivlanassoc=24,44
```

CREATE MSTP

Syntax

```
create mstp mstiid=mstiid [mstivlanassoc=vids]
```

Parameters

mstiid	Specifies the MSTI ID of the spanning tree instance you want to create. You can specify only one MSTI ID at a time. The range is 1 to 15.
mstivlanassoc	Specifies the VID of the VLAN you want to associate with the MSTI ID. You can specify more than one VID at a time (for example, 2,5,44).

Description

This command creates an MSTI ID and associates VLANs to the new spanning tree instance.

The MSTIID parameter specifies the new MSTI ID.

The MSTIVLANASSOC parameter specifies the VIDs of the VLANs you want to associate with the new MSTI. The VLANs must already exist on the switch. If you do not specify any VLANs, you can add them later using “ADD MSTP” on page 491 or “SET MSTP MSTIVLANASSOC” on page 504.

Examples

The following command creates the MSTI ID 8 and associates to it the VLAN with the VID 4:

```
create mstp mstiid=8 mstivlanassoc=4
```

The following command creates the MSTI ID 11 and associates to it the VLANs with the VIDs 24 and 44:

```
create mstp mstiid=11 mstivlanassoc=24,44
```

DELETE MSTP

Syntax

```
delete mstp mstiid=mstiid mstivlanassoc=vids
```

Parameters

mstiid	Specifies the MSTI ID of the spanning tree instance where you want to remove VLANs. You can specify only one MSTI ID at a time. The range is 1 to 15.
mstivlanassoc	Specifies the VID of the VLAN you want to remove from the spanning tree instance. You can specify more than one VID at a time (for example, 2,5,44).

Description

This command removes a VLAN from a spanning tree instance. A VLAN removed from a spanning tree instance is automatically returned to CIST.

The MSTIID parameter specifies the MSTI ID.

The MSTIVLANASSOC parameter specifies the VIDs of the VLANs you want to remove from the spanning tree instance.

Examples

The following command deletes the VLAN with the VID 4 from MSTI ID 8:

```
delete mstp mstiid=8 mstivlanassoc=4
```

The following command deletes the VLANs with the VIDs 24 and 44 from MSTI ID 11:

```
delete mstp mstiid=11 mstivlanassoc=24,44
```

DESTROY MSTP MSTIID

Syntax

```
destroy mstp mstiid=mstiid
```

Parameter

mstiid	Specifies the MSTI ID of the spanning tree instance you want to delete. You can specify only one MSTI ID at a time. The range is 1 to 15.

Description

This command deletes a spanning tree instance. VLANs associated with a deleted MSTI are returned to CIST.

Example

The following command deletes the spanning tree instance 4:

```
destroy mstp mstiid=4
```

DISABLE MSTP

Syntax

```
disable mstp
```

Parameters

None.

Description

This command disables the Multiple Spanning Tree Protocol on the switch. To view the current status of MSTP, refer to "SHOW MSTP" on page 509.

Example

The following command disables MSTP:

```
disable mstp
```

ENABLE MSTP

Syntax

```
enable mstp
```

Parameters

None.

Description

This command enables Multiple Spanning Tree Protocol on the switch. To view the current status of MSTP, refer to “SHOW MSTP” on page 509.

You must select MSTP as the active spanning tree on the switch before you can enable it with this command. To activate MSTP, see “ACTIVATE MSTP” on page 490.

Example

The following command enables MSTP:

```
enable mstp
```

PURGE MSTP

Syntax

```
purge mstp
```

Parameters

None.

This command returns all MSTP bridge and port parameters settings to their default values. This command also deletes all multiple spanning tree instances and VLAN associations.

In order for you to use this command, MSTP must be the active spanning tree protocol on the switch and the protocol must be disabled. To select MSTP as the active spanning tree protocol on the switch, see "ACTIVATE MSTP" on page 490. To disable MSTP, refer to "DISABLE MSTP" on page 495.

Example

The following command resets the MSTP bridge and port parameter settings:

```
purge mstp
```

Equivalent Command

```
set mstp default
```

For information, see "SET MSTP" on page 498.

SET MSTP

Syntax

```
set mstp [default]
[forceversion=stpcompatible|forcestpcompatible|
normalmstp] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
[maxhops=maxhops] [configname="name"]
[revisionlevel=number]
```

Parameters

default — Disables MSTP and returns all bridge and port MSTP settings to the default values. This parameter cannot be used with any other parameter. (This parameter performs the same function as the PURGE MSTP command.) The spanning tree protocol must be disabled to use this parameter.

forceversion — Controls whether the bridge will operate with MSTP or in an STP-compatible mode. If you select MSTP, the bridge will operate all ports in MSTP, except for those ports that receive STP or RSTP BPDU packets. If you select STP Compatible or Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports

The options are:

stpcompatible ***or*** forcestpcompatible	The bridge uses the MSTP parameter settings, but transmits only STP BPDU packets from the ports. These options are equivalent.
normalmspt	The bridge uses MSTP. The bridge sends out MSTP BPDU packets from all ports except for those ports connected to bridges running STP. This is the default setting.

hellotime — Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

forwarddelay — Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The default is 15 seconds. This parameter effects only those ports operating in the STP compatible mode.

maxage — Specifies the length of time, in seconds, after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

Note
The value for the maxage parameter must be greater than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

maxhops — Specifies the maximum hops counter. MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses a bridge within a MSTP region. After the counter reaches zero, the BPDU is deleted. The counter is reset to its original value if the BPDU crosses a MSTP regional boundary.

configname — Specifies the name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters. The name is case-sensitive and must be the same on all bridges in a region. Examples include Sales Region and Production Region. The name must be enclosed in quotes.

revisionlevel — Specifies the reversion number of an MSTP region. The range is 0 (zero) to 255. This is an arbitrary number that you assign to a region. The reversion level must be the same on all bridges in a region. Different regions can have the same reversion level without conflict.

Description

This command configures the following MSTP parameter settings.

- Hello time
- Forwarding delay
- Maximum age time

- Maximum hop count
- Force version of STP or normal MSTP
- Configuration name
- Revision level

Examples

The following command disables MSTP and returns all MSTP parameter settings to their default values:

```
set mstp default
```

The following command sets the hop count to 10, the configuration name to Engineering Region, and the reversion level to 2:

```
set mstp maxhops=10 configname="Engineering Region"
revisionlevel=2
```

The following command uses the FORCEVERSION parameter to configure the bridge to use the MSTP parameters but to transmit only STP BPDU packets:

```
set mstp forceversion=forcestpcompatible
```

Equivalent Command

```
purge mstp
```

For information, see “PURGE MSTP” on page 497. This command performs the same function as the DEFAULT parameter.

SET MSTP CIST

Syntax

```
set mstp cist priority=priority
```

Parameter

priority — Specifies the CIST priority number for the switch. The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 20. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 20. CIST Priority Value Increments

Increment	CIST Priority	Increment	CIST Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Description

This command sets the CIST priority number on the switch. This number is used in determining the root bridge for the bridged network. The bridge with the lowest priority number acts as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. To view the current CIST priority number, see "SHOW MSTP" on page 509.

Example

The following command sets the CIST priority value to 45,056, which is increment 11:

```
set mstp cist priority=11
```

SET MSTP MSTI

Syntax

```
set mstp msti mstiid=mstiid priority=priority
```

Parameters

mstiid — Specifies a MSTI ID. You can specify only one MSTI ID at a time. The range is 1 to 15.

priority — Specifies the MSTI priority value for the switch. The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 21. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 21. MSTI Priority Value Increments

Increment	MSTI Priority	Increment	MSTI Priority
0	0	8	32,768
1	4,096	9	36,864
2	8,192	10	40,960
3	12,288	11	45,056
4	16,384	12	49,152
5	20,480	13	53,248
6	24,576	14	57,344
7	28,672	15	61,440

Description

This command changes the MSTI priority value of a spanning tree instance on a bridge. This value is used in determining the regional root bridge of a spanning tree instance.

The MSTIID parameter specifies the MSTI ID whose MSTI priority you want to change. The range is 1 to 15.

The PRIORITY parameter specifies the new MSTI priority value. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority.

Examples

The following command changes the MSTI priority value to 45,056 (increment 11) for the MSTI ID 4:

```
set mstp msti mstiid=4 priority=11
```

The following command changes the MSTI priority value to 8,192 (increment 2) for the MSTI ID 6:

```
set mstp msti mstiid=6 priority=2
```

SET MSTP MSTIVLANASSOC

Syntax

```
set mstp mstivlanassoc mstiid=mstiid vlanlist=vids
```

Parameters

mstiid	Specifies the ID of the spanning tree instance where you want to associate VLANs. You can specify only one MSTI ID at a time. The range is 1 to 15.
vlanlist	Specifies the VID of the VLAN you want to associate with the MSTI ID. You can specify more than one VID at a time (for example, 2,5,44). If VLANs have already been associated with the MSTI, they are overwritten.

Description

This command associates VLANs to spanning tree instances.

The MSTIID parameter specifies the ID of the spanning tree instance. The spanning tree instance must already exist on the switch. To create a spanning tree instance, see “CREATE MSTP” on page 492.

The VLANLIST parameter specifies the VID of the VLANs you want to associate with the MSTI. The VLANs must already exist on the switch. If VLANs are already associated with the MSTI, they are removed and returned to CIST. If you want to add VLANs to an MSTI and retain those VLANs already associated with it, see “ADD MSTP” on page 491.

Examples

The following command associates the VLAN with the VID 4 to MSTI ID 8:

```
set mstp mstivlanassoc mstiid=8 vlanlist=4
```

The following command associates VIDs 24 and 44 to MSTI ID 11:

```
set mstp mstivlanassoc mstiid=11 vlanlist=24,44
```

SET MSTP PORT

Syntax 1

```
set mstp port=port|all [extportcost=portcost]
[edgeport=yes|no|no|on|off|true|false]
[ptp|pointtopoint=yes|no|on|off|true|false|autoupdate]
[migrationcheck=yes|no|on|off|true|false]
```

Syntax 2

```
set mstp port=port|all [intportcost=auto|portcost]
[portpriority=priority] [stpid=msti_id]
```

Parameters

port — Specifies the port you want to configure. You can specify more than one port at a time. To configure all ports in the switch, enter ALL.

extportcost — Specifies the cost of a port connected to a bridge that is a member of another MSTP region or is running STP or RSTP. This is referred to as an external port cost. The range is 0 to 200,000,000. The default setting is Auto, which sets port cost based on port speed. Table 22 lists the MSTP external port costs with the Auto setting when the port is not a member of a trunk.

Table 22. Auto External Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 23 lists the MSTP port costs with the Auto setting when the port is part of a port trunk.

Table 23. Auto External Path Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

edgeport — Defines whether the port is functioning as an edge port. An edge port is connected to a device operating at half-duplex mode and is not connected to any device running STP or MSTP. Selections are:

- yes, on, true — The port is an edge port. These values are equivalent. This is the default.
- no, off, false — The port is not an edge port. These values are equivalent.

ptp ***or*** pointtopoint — Defines whether the port is functioning as a point-to-point port. This type of port is connected to a device operating at full-duplex mode. Selections are:

- yes, on, true — The port is an point-to-point port.
- no, off, false — The port is not an point-to-point port.
- autoupdate — The port's status is determined automatically. This is the default.

migrationcheck — This parameter resets a MSTP port, allowing it to send MSTP BPDUs. When a MSTP bridge receives STP BPDUs on an MSTP port, the port transmits STP BPDUs. The MSTP port continues to transmit STP BPDUs indefinitely. Set the migrationcheck parameter to yes to reset the MSTP port to transmit MSTP BPDUs.

- yes, on, true — Enable migration check. The values are equivalent.
- no, off, false — Disable migration check. The values are equivalent.

Note
Each time a MSTP port is reset by receiving STP BPDUs, set the migrationcheck parameter to yes, allowing the port to send MSTP BPDUs.

intportcost — Specifies the cost of a port connected to a bridge that is part of the same MSTP region. This is referred to as an internal port cost. The range is 0 to 200,000,000. The default setting is Auto-detect (0), which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

portpriority — Specifies the port's priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. There are sixteen increments, as shown in Table 24 on page 507. You specify the increment of the desired value. The default is 128, which is increment 8.

Table 24. Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

stpid — Specifies the ID number of an MSTI in which the VLAN of a port is a member. This parameter is used with the INTPORTCOST and PORTPRIORITY parameters to assign different path costs and priority values to untagged and tagged ports whose VLANs belong to more than one MSTI. You can specify more than one MSTI at a time (e.g., 4,6,11). If the VLANs of a port belong to just one MSTI, you can omit this parameter.

Description

This command sets a port's MSTP settings. The command is illustrated in two syntaxes to represent the two groups of MSTI port parameters. The first group is referred to as generic parameters. They are set just once on a port, regardless of the number of MSTIs where a port is a member. These parameters are the external path cost and edge port and point-to-point port designations.

The second group can be applied independently on a port on a per-MSTI basis. There are two parameters in this group — internal path cost and priority. A port whose VLANs are members of different MSTIs can have different settings in each MSTI. The MSTI is identified with the STPID parameter. You can omit the STPID parameter if a port is a member of one or more VLANs that all belong to the same MSTI, or if you want to assign the port the same path cost or priority value in all of its MSTI assignments.

Synax 1 Examples

The following command sets the external port cost to 500 for Ports 14 and 23:

```
set mstp port=14,23 extportcost=500
```

The following command sets the external port cost to 1,000,000 for Port 4 and designates it as an edge port:

```
set mstp port=6-8 edgeport=yes
```

The following command sets the external port cost for Ports 2 and 5 to Auto, which sets the port cost based on speed:

```
set mstp port=2-5 extportcost=auto
```

The following command designates Ports 6 to 8 as point-to-point ports:

```
set mstp port=6-8 ptp=yes
```

Syntax 2 Examples

The following command sets the internal port cost to 500 for Ports 7 and 10. If the ports are members of more than one VLAN and the VLANs are assigned to more than one MSTI, the new internal port cost is assigned to all of their MSTI assignments:

```
set mstp port=7,10 intportcost=500
```

This example illustrates the STPID parameter. This parameter is used when a port belongs to more than one VLAN and the VLANs are assigned to different MSTIs. You can use the parameter to specify different priority and internal port costs on a port for each MSTI assignment. This command assigns Port 15 in MSTI 2 a priority of 64 (increment 4):

```
set mstp port=7,10 portpriority=4 stpid=2
```

The following command sets the internal port cost to 1,000,000 and port priority to 224 (increment 14) for Port 4:

```
set mstp port=4 intportcost=1000000 portpriority=14
```

The following command is similar to the previous example, except it assumes port 4 is a member of more than one MSTI and you want to assign the new values to only one of its MSTI assignments, in this case MSTI 12:

```
set mstp port=4 intportcost=1000000 portpriority=14 stpid=12
```

The following command sets the internal port cost for Ports 2 and 5 to Auto, which sets the port cost based on speed:

```
set mstp port=2-5 intportcost=auto
```

SHOW MSTP

Syntax

```
show mstp [portconfig=ports] [portstate=ports]
[stpid=msti_id] [mstistate] [cist] [mstivlanassoc]
```

Parameters

portconfig	Displays the MSTP settings of a port. You can specify more than one port at a time. For a list of the MSTP information displayed by this parameter, refer to Description below.
portstate	Displays the MSTP state of a port. You can specify more than one port at a time. For a list of the MSTP information displayed by this parameter, refer to Description below.
stpid	Specifies an MSTI ID. This parameter is used with the PORTCONFIG and PORTSTATE parameters to view MSTP settings for a port whose VLANs are members of different MSTIs. You can specify more than one MSTI ID.
mstistate	Displays a list of the MSTIs on the switch and their associated VLANs. The list does not include the CIST.
cist	Displays the CIST priority and the VLANs associated with CIST.
mstivlanassoc	Displays a list of the MSTIs on the switch, including the CIST, and their associated VLANs.

Note
You can specify only one parameter at a time in this command. The only exception is the STPID parameter, which can be used together with the PORTCONFIG and PORTSTATE parameters.

Description

This command displays MSTP parameters. For definitions of the MSTP terms used below, refer to Chapter 24, "Multiple Spanning Tree Protocol" in the *AT-S63 Management Software Menus Interface User's Guide*.

Entering SHOW MSTP without any parameters displays the following MSTP settings:

- MSTP status
- Force version
- Hello time
- Forwarding delay
- Maximum age
- Maximum hops
- Configuration name
- Reversion level
- Bridge identifier
- Root identifier

The hello time, forwarding delay, and bridge max age parameters will have two values if MSTP is enabled on the switch (for example, Forwarding Delay .. 15/15). The first number is the configured value on the switch for the parameter and the second is the value the switch obtained from the root bridge and is actually using for the parameter. The switch displays only the configured values for these parameters if spanning tree is not enabled on the switch.

The bridge Identifier parameter consists of the switch's CIST priority value and MAC address, separated by a slash (/). To change the CIST priority value, refer to "SET MSTP CIST" on page 501. The MAC address of the switch cannot be changed.the MAC address of the switch.

The root bridge parameter specifies the bridge identifier of the root bridge of the spanning tree domain. The identifier consists of the bridge or CIST priority value and MAC address of the root switch, separated by a slash (/). This parameter only appears when STP is activated on the switch.

The PORTCONFIG parameter displays the following MSTP port parameter settings:

- Edge-port status
- Point-to-point status
- External and internal port costs
- Port priority

The PORTSTATE parameter displays the following MSTP port status information:

- MSTP port state
- MSTP role

- Point-to-point status
- Spanning tree version
- Internal and external port costs

The MSTI parameter displays the following information for each spanning tree instance (excluding the CIST) on the switch:

- MSTI ID
- MSTI priority
- Regional root ID
- Path cost
- Associated VLANs

The CIST parameter displays the following CIST information:

- CIST priority value
- Root ID
- Root path cots
- Regional root ID
- Regional root path cost
- Associated VLANs

The MSTIVLANASSOC parameter displays the VLAN to MSTI associations.

Examples

This command displays basic MSTP operating information:

```
show mstp
```

This command displays the MSTP state of Port 4:

```
show mstp portstate=4
```

This command displays the configuration of Port 5 in MSTI 2:

```
show mstp portconfig=5 stpid=2
```

This command displays the CIST information:

```
show mstp cist
```

This command displays the VLAN associations:

```
show mstp mstivlanassoc
```

Section VI

Virtual LANs

The chapters in this section contain the commands for managing virtual LANs using the AT-S63 management software. The chapters include:

- Chapter 29, “Port-based, Tagged, and Multiple Mode VLAN Commands” on page 515
- Chapter 30, “GARP VLAN Registration Protocol Commands” on page 533
- Chapter 31, “Protected Ports VLAN Commands” on page 547
- Chapter 32, “MAC Address-based VLAN Commands” on page 557

Chapter 29

Port-based, Tagged, and Multiple Mode VLAN Commands

This chapter contains the following commands:

- "ADD VLAN" on page 516
- "CREATE VLAN" on page 518
- "DELETE VLAN" on page 521
- "DESTROY VLAN" on page 523
- "SET SWITCH INFILTERING" on page 524
- "SET SWITCH MANAGEMENTVLAN" on page 525
- "SET SWITCH VLANMODE" on page 526
- "SET VLAN" on page 528
- "SHOW VLAN" on page 529

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
For background information on tagged and port-based VLANs, and ingress filtering, refer to Chapter 25, "Port-based and Tagged VLANs" in the *AT-S63 Management Software Menus Interface User's Guide*. For background information about the multiple VLAN modes, refer to Chapter 27, "Multiple VLAN Modes" in the *AT-S63 Management Software Menus Interface User's Guide*.

ADD VLAN

Syntax 1

```
add vlan=name [vid=vid] ports=ports|all
frame=untagged|tagged
```

Syntax 2

```
add vlan=name [vid=vid] taggedports=ports|all
untaggedports=ports|all
```

Parameters

vlan	Specifies the name of the VLAN to modify.
vid	Specifies the VID of the VLAN you want to modify. This parameter is optional.
ports	Specifies the ports to be added to the VLAN. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).
frame	Identifies the new ports as either tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the ports to be added as tagged ports to the VLAN. To include all ports on the switch as tagged ports in the VLAN, use ALL.
untaggedports	Specifies the ports to be added as untagged ports to the VLAN. Specifying ALL adds all ports on the switch as untagged ports to the VLAN.

Description

This command adds tagged and untagged ports to an existing port-based or tagged VLAN.

Note
To initially create a VLAN, see “CREATE VLAN” on page 518. To remove ports from a VLAN, see “DELETE VLAN” on page 521.

This command has two syntaxes. You can use either command to add ports to a VLAN. The difference between the two is that Syntax 1 can add only one type of port, tagged or untagged, at a time to a VLAN, while Syntax 2 can add both in the same command. This is illustrated in Examples below.

When you add untagged ports to a VLAN, the ports are automatically removed from their current untagged VLAN assignment. This is because a port can be an untagged member of only one VLAN at a time. For example, if you add port 4 as an untagged port to a VLAN, the port is automatically removed from whichever VLAN it is currently an untagged member.

Adding a tagged port to a VLAN does not change the port's current tagged and untagged VLAN assignments. This is because a tagged port can belong to more than one VLAN at a time. For instance, if you add port 6 as an tagged port to a new VLAN, port 6 remains a tagged and untagged member of its other VLAN assignments.

Examples

The following command uses Syntax 1 to add ports 4 and 7 as untagged members to a VLAN called Sales:

```
add vlan=sales ports=4,7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
add vlan=sales untaggedports=4,7
```

The following command uses Syntax 1 to add port 3 as a tagged member to a VLAN called Production:

```
add vlan=production ports=3 frame=tagged
```

The following command does the same thing using Syntax 2:

```
add vlan=production untaggedports=3
```

Adding both tagged and untagged ports to a VLAN using Syntax 1 takes two commands, one command for each port type. For example, if you had a VLAN called Service and you wanted to add port 5 as a tagged port and ports 7 and 8 as untagged ports, the commands would be:

```
add vlan=Service ports=5 frame=tagged
```

```
add vlan=Service ports=7-8 frame=untagged
```

Using Syntax 2, you can add both types of ports with just one command:

```
add vlan=Service untaggedports=7-8 taggedports=5
```

CREATE VLAN

Syntax 1

```
create vlan=name vid=vid [type=port] ports=ports|all
frame=untagged|tagged
```

Syntax 2

```
create vlan=name vid=vid [type=port] taggedports=ports|all
untaggedports=ports|all
```

Parameters

vlan

Specifies the name of the VLAN. You must assign a name to a VLAN.

The name can be from 1 to 20 characters in length and should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

The name cannot be the same as the name of an existing VLAN on the switch.

If the VLAN is unique in your network, then the name needs to be unique as well. If the VLAN spans multiple switches, then the name for the VLAN should be the same on each switch.

vid

Specifies the VLAN identifier. The range is 2 to 4094. The VLAN must be assigned a VID.

You cannot use the VID 1, which is reserved for the Default_VLAN.

The VID cannot be the same as the VID of an existing VLAN on the switch.

If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, assign the Sales VLAN on each switch the same VID value.

type	Specifies the type of VLAN to be created. The option PORT signifies a port-based or tagged VLAN. This parameter is optional.
ports	Specifies the ports on the switch that are either tagged or untagged members of the new VLAN. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22). To specify all ports on the switch, use ALL. This parameter must be followed by the FRAME parameter.
frame	Specifies whether the ports of the VLAN are to be tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the ports on the switch to serve as tagged ports in the VLAN. To specify all ports on the switch, use ALL. Omit this parameter if the VLAN does not contain tagged ports.
untaggedports	Specifies the ports on the switch to function as untagged ports in the VLAN. To specify all ports on the switch, use ALL. Omit this parameter if the VLAN does not contain untagged ports.

Description

This command creates a port-based or tagged VLAN.

This command has two syntaxes. You can use either syntax to create a port-based or tagged VLAN. The difference between the two syntaxes is how you specify which ports are members of the VLAN and whether the ports are tagged or untagged. Syntax 1 is limited because it allows you to specify either tagged or untagged ports, but not both at the same time. On the other hand, you can use Syntax 2 to create a VLAN that has both types of ports. This is illustrated in the Examples section below.

When you create a new VLAN, untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. This is because a port can be an untagged member of only one VLAN at a time. For example, creating a new VLAN with untagged Ports 1 to 4 automatically removes these ports from whichever VLAN they are currently untagged members.

The PVID of an untagged port is automatically changed to match the VID number of the VLAN to which it is added. For instance, if you make port 4 an untagged member of a VLAN with a VID of 15, port 4's PVID is changed to 15 automatically.

Tagged ports of the new VLAN remain as tagged and untagged members of their current VLAN assignments. No change is made to a tagged port's current VLAN assignments, other than its addition to the new VLAN. This is because a tagged port can belong to more than one VLAN at a time. For example, if you add port 6 as a tagged port to a new VLAN, port 6 remains a member of its other current untagged and tagged VLAN assignments.

Examples

The following command uses Syntax 1 to create a port-based VLAN called Sales with a VID of 3. The VLAN will consist of ports 4 to 8 and ports 12 to 16. All ports will be untagged ports in the VLAN:

```
create vlan=Sales vid=3 ports=4-8,12-16 frame=untagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan=Sales vid=3 untaggedports=4-8,12-16
```

In the following command, Syntax 1 is used to create a tagged VLAN called Production with a VID of 22. The VLAN will consist of two tagged ports, ports 3 and 6:

```
create vlan=Production vid=22 ports=3,6 frame=tagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan=Sales vid=22 taggedports=3,6
```

You cannot use Syntax 1 to create a tagged VLAN that contains both untagged and tagged ports. For instance, suppose you wanted to create a VLAN called Service with a VID of 16 and untagged ports 1, 4, 5-7 and tagged ports 11 and 12. Creating this VLAN using Syntax 1 would actually require two commands. You would first need to create the VLAN, specifying either the untagged or tagged ports. As an example, the following command creates the VLAN and specifies the untagged ports:

```
create vlan=Service vid=16 ports=1,4,5-7 frame=untagged
```

Then, to add the other ports (in this case tagged ports), you would need to use the ADD VLAN command.

Syntax 2 allows you to create a VLAN of both tagged and untagged ports all in one command. Here is the command that would create our example:

```
create vlan=Service vid=16 untaggedports=1,4,5-7
taggedports=11-12
```

The advantage of Syntax 2 over Syntax 1 is that you can create VLANs containing both types of ports with one rather than two commands.

DELETE VLAN

Syntax 1

```
delete vlan=name [vid=vid] ports=ports frame=untagged|tagged
```

Syntax 2

```
delete vlan=name [vid=vid] taggedports=ports
untaggedports=ports
```

Parameters

vlan	Specifies the name of the VLAN to be modified.
vid	Specifies the VID of the VLAN to be modified. This parameter is optional.
ports	Specifies the ports to be removed from the VLAN. This parameter must be used with the FRAME parameter.
frame	Identifies the ports to be removed as tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the tagged ports to be removed from the VLAN.
untaggedports	Specifies the untagged ports to be removed from the VLAN.

Description

This command removes tagged and untagged ports from a port-based or tagged VLAN.

This command has two syntaxes. You can use either command to delete ports from a VLAN. The difference between the two is that Syntax 1 can remove only one type of port, tagged or untagged, at a time from a VLAN, while Syntax 2 allows you to remove both port types in the same command. This is illustrated in the Examples section below.

Note
To delete a VLAN, see "DESTROY VLAN" on page 523.

Note
You cannot change a VLAN's name or VID.

When you remove an untagged port from a VLAN, the following happens:

- The port is returned to the Default_VLAN as an untagged port.
- If the port is also a tagged member of other VLANS, those VLAN assignments are not changed. The port remains a tagged member of the other VLANs. For example, if you remove Port 4 from a VLAN, the port is automatically returned as an untagged port to the Default VLAN. If Port 4 is functioning as a tagged member in one or more other VLANs, it remains as a tagged member of those VLANs.
- If you remove an untagged port from the Default_VLAN without assigning it to another VLAN, the port is excluded as an untagged member from all VLANs on the switch.

When you remove a tagged port from a VLAN, all of its other tagged and untagged VLAN assignments remain unchanged.

Examples

The following command uses Syntax 1 to delete untagged ports 4 and 7 from a VLAN called Sales:

```
delete vlan=sales ports=4,7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
delete vlan=sales untaggedports=4,7
```

The following command uses Syntax 1 to delete tagged port 13 from a VLAN called Production:

```
delete vlan=production ports=13 frame=tagged
```

The following command does the same thing using Syntax 2:

```
delete vlan=production untaggedports=13
```

To delete both tagged and untagged ports from a VLAN using Syntax 1 takes two commands. For example, if you had a VLAN called Service and you wanted to delete from the VLAN tagged port 2 and untagged ports 6 to 8, the commands would be:

```
delete vlan=Service ports=2 frame=tagged

delete vlan=Service ports=6-8 frame=untagged
```

Using Syntax 2, you can do the whole thing with just one command:

```
delete vlan=Service untaggedports=6-8 taggedports=2
```

DESTROY VLAN

Syntax

```
destroy vlan=name|vid|all
```

Parameters

vlan	Specifies the name or VID of the VLAN to be deleted. To delete all VLANs, use the ALL option.

Description

This command deletes port-based, tagged, and MAC address-based VLANs from a switch. You can use the command to deleted selected VLANs or all VLANs, with the exception of the Default_VLAN.

Examples

The following command deletes the Sales VLAN from the switch:

```
destroy vlan=Sales
```

The following command deletes the Sales VLAN using both the name and the VID:

```
destroy vlan=Sales vid=102
```

The following command deletes all port-based and tagged VLANs on a switch:

```
destroy vlan=all
```

SET SWITCH INFILTERING

Syntax

```
set switch infiltering=yes|no|on|off|true|false
```

Parameters

infiltering — Specifies the operating status of ingress filtering. The options are:

- yes, on, true — Activates ingress filtering. The options are equivalent. This is the default.
- no, off, false — Deactivates ingress filtering. The options are equivalent.

Description

This command controls the status of ingress filtering. When ingress filtering is activated, which is the default, tagged frames are filtered when they are received on a port. When ingress filtering is deactivated, tagged frames are filtered before they are transmitted out a port. To view the current setting, use the “SHOW SWITCH” on page 76. For further information on ingress filtering, refer to the *AT-S63 Management Software Menus Interface User’s Guide*.

Example

The following command deactivates ingress filtering:

```
set switch infiltering=off
```

SET SWITCH MANAGEMENTVLAN

Syntax

```
set switch managementvlan=name|VID
```

Parameter

managementvlan	Specifies the management VLAN. You can specify the VLAN by name or by its VID. You can specify only one management VLAN. The default management VLAN is Default_VLAN (VID 1).

Description

This command sets the management VLAN. The switch uses this VLAN to watch for management packets from remote Telnet, SSH, and web browser management sessions. For background information on the function of the management VLAN, refer to Chapter 25, "Port-based and Tagged VLANs" in the *AT-S63 Management Software Menus Interface User's Guide*. To determine the current management VLAN, use the SHOW SWITCH command.

Example

The following command sets the TechSupport VLAN as the management VLAN:

```
set switch managementvlan=TechSupport
```

SET SWITCH VLANMODE

Syntax

```
set switch vlanmode=userconfig|dotqmultiple|multiple
[uplinkport=port]
```

Parameters

vlanmode — Controls the switch's VLAN mode. Options are:

- userconfig — This mode allows you to create your own port-based and tagged VLANs. This is the default setting.
- dotqmultiple — This option configures the switch for the 802.1Q-compliant multiple VLAN mode.
- multiple — This option configures the switch for the non-802.1Q compliant multiple VLAN mode.

uplinkport — Specifies the port on the switch to function as the uplink port when the switch is operating in one of the two multiple VLAN modes. You can specify only one port.

Description

You use this command to configure the switch for one of the multiple VLAN modes or so that you can create port-based and tagged VLANs.

If you select one of the multiple VLAN modes, you must also set an uplink port with the UPLINKPORT parameter. You can specify only one uplink port.

Note
For background information on the multiple VLAN modes, refer to Chapter 27, "Multiple VLAN Modes" in the *AT-S63 Management Software Menus Interface User's Guide*.

Examples

The following command configures the switch for the 802.1Q-compliant multiple VLAN mode and specifies port 4 as the uplink port:

```
set switch vlanmode=dotqmultiple uplinkport=4
```

The following command sets the switch so that you can create your own port-based and tagged VLANs:

```
set switch vlanmode=userconfig
```

SET VLAN

Syntax

```
set vlan=name [vid=vid] type=portbased
```

Parameter

vlan	Specifies the name of the dynamic GVRP VLAN you want to convert into a static VLAN. To view VLAN names, refer to “SHOW VLAN” on page 529.
vid	Specifies the VID of the dynamic VLAN. To view VIDs, refer to “SHOW VLAN” on page 529. This parameter is optional.
type	Specifies the type of static VLAN to which the dynamic VLAN is to be converted. There is only one option: PORTBASED.

Description

This command converts a dynamic GVRP VLAN into a static tagged VLAN. You can perform this command to permanently retain the VLANs the switch learned through GVRP.

Note
This command cannot convert a dynamic GVRP port in a static VLAN into a static port. For that you must manually modify the static VLAN, specifying the dynamic port as either a tagged or untagged member of the VLAN.

Example

This command changes the dynamic VLAN GVRP_VLAN_22 into a static VLAN:

```
set vlan=gvrp_vlan_22 type=portbased
```

SHOW VLAN

Syntax

```
show vlan[=name|vid]
```

Parameter

vlan — Specifies the name or VID of the VLAN.

Description

This command displays the VLANs on the switch. An example of the information displayed by this command for port-based and tagged VLANs is shown in Figure 51.

```
VLAN Name ............................ Sales
VLAN ID .............................. 4
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s)
  Configured ......................... 2,8-12
  Actual ............................. 2,8-12
Tagged Port(s) ....................... 24

VLAN Name ............................ Engineering
VLAN ID .............................. 5
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s)
  Configured ......................... 5-7
  Actual ............................. 5-7
Tagged Port(s) ....................... 24
```

Figure 51. SHOW VLAN Command for Port-based and Tagged VLANs

The information displayed by the command is described here:

- VLAN name - The name of the VLAN.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be Port Based for port-based and tagged VLANs.
- Protected Ports - The status of protected ports. Since port-based and tagged VLANs are not protected ports VLANs, this will be No.
- Untagged port(s) - The untagged ports of the VLAN. The untagged ports are listed as follows.
  - Configured: The untagged ports assigned to the VLAN when the VLAN was created or modified.

– Actual: The current untagged ports of the VLAN. If you are not using 802.1x port-based network access control, both the Configured and Actual untagged ports of a VLAN will always be the same.

  If you are using 802.1x and you assigned a guest VLAN to an authenticator port or you associated an 802.1x supplicant to a VLAN on the authentication server, it is possible for ports to be in different VLANs than the virtual LANs where they were originally assigned as untagged ports. In these situations, the Configured and Actual port lists can differ, with the Actual list detailing the ports that are currently functioning as untagged ports of the VLAN.

  For example, if a particular port is listed as a Configured member of a VLAN, but not as an Actual member, that would mean either the port is currently a part of a Guest VLAN or the supplicant who logged on the port was associated with a VLAN assignment on the authentication server.

❒ Tagged port(s) - The tagged ports of the VLAN. A tagged port can belong to more than one VLAN at a time.

An example of the information displayed by this command for the 802.1Q-compliant multiple VLAN mode is shown in Figure 52.

```
VLAN Mode: Pre Configured (802.1Q Multiple VLANs)
VLAN Information:

VLAN Name ............................ Client_VLAN_1
VLAN ID .............................. 1
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s) ..................... 1
Tagged Port(s) ....................... 23

VLAN Name ............................ Client_VLAN_2
VLAN ID .............................. 2
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s) ..................... 2
Tagged Port(s) ....................... 23

VLAN Name ............................ Client_VLAN_3
VLAN ID .............................. 3
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s) ..................... 3
Tagged Port(s) ....................... 23
```

Figure 52. SHOW VLAN Command for the 802.1Q-compliant Multiple VLAN Mode

The information displayed by the command is described here:

- VLAN name - The name of the VLAN. The name is Client_VLAN followed by the port number.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be Port Based for the VLANs of a multiple VLAN mode.
- Protected Ports - The status of protected ports. Since the VLANs of a multiple VLAN mode are not protected ports VLANs, this will be No.
- Untagged port(s) - The untagged port of the VLAN.
- Tagged port(s) - The tagged port that is functioning as the uplink port for the VLANs.

For an example of the information displayed by this command for a protected ports VLAN, see Figure 53 on page 555. For an example of a MAC address-based VLAN, see Figure 54 on page 565.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays information on just the Sales VLAN:

```
show vlan=sales
```

The following command displays information for the VLAN with the VID of 22:

```
show vlan=22
```

Chapter 30

GARP VLAN Registration Protocol Commands

This chapter contains the following commands:

- “DISABLE GARP” on page 534
- “ENABLE GARP” on page 535
- “PURGE GARP” on page 536
- “SET GARP PORT” on page 537
- “SET GARP TIMER” on page 538
- “SHOW GARP” on page 540
- “SHOW GARP COUNTER” on page 541
- “SHOW GARP DATABASE” on page 543
- “SHOW GARP GIP” on page 544
- “SHOW GARP MACHINE” on page 545

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 26, “GARP VLAN Registration Protocol” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE GARP

Syntax

```
disable garp=gvrp [gip]
```

Parameters

garp	Specifies the GARP application you want to disable. The only GARP application supported by AT-S63 management software is GVRP.
gip	Disables GARP Information Propagation (GIP).

Note
The online help for this command contains an STP option. The option is not supported.

Description

This command disables GVRP on the switch. After disabled, the switch will not learn any new dynamic GVRP VLANs or dynamic GVRP ports.

You can also use this command to disable GIP.

Note
Do not disable GIP if the switch is running GVRP. GIP is required for proper GVRP operation.

Examples

The following command disables GVRP on the switch:

```
disable garp=gvrp
```

The following command disables GIP only:

```
disable garp=gvrp gip
```

ENABLE GARP

Syntax

```
enable garp=gvrp [gip]
```

Parameters

garp	Specifies the GARP application you want to enable. The only GARP application supported by AT-S63 management software is GVRP.
gip	Enables GARP Information Propagation (GIP).

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command enables GVRP on the switch. After activated, the switch will learn dynamic GVRP VLANs and dynamic GVRP ports.

You can also use this command to enable GIP. GIP must be enabled for GVRP to operate properly.

Examples

The following command enables GVRP on the switch:

```
enable garp=gvrp
```

The following command enables GIP only:

```
enable garp=gvrp gip
```

PURGE GARP

Syntax

```
purge garp=gvrp
```

Parameter

garp	Specifies the GARP application you want to reset. The only GARP application supported by AT-S63 management software is GVRP.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command disables GVRP and returns all GVRP parameters to their default settings. All GVRP-related statistics counters are returned to zero.

Example

The following command disables GVRP and returns all GVRP parameters to their default values:

```
purge garp=gvrp
```

SET GARP PORT

Syntax

```
set garp=gvrp port=port mode=normal|none
```

Parameters

garp — Specifies the GARP application you want to configure. The only GARP application supported by AT-S63 management software is GVRP.

port — Specifies the port you want to configure on the switch. You can specify more than one port at a time.

mode — Specifies the GVRP mode of the port. Modes are:

- normal — The port will participate in GVRP. The port will process GVRP information and transmit PDUs. This is the default.
- none — The port will not participate in GVRP. The port will not process GVRP information nor transmit PDUs.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command sets a port's GVRP status. If you want a port to learn remote VLANs and transmit PDUs, set its mode to Normal. If you do not want a port to participate in GVRP, set its mode to None.

Examples

The following command sets ports 1 to 4 to not participate in GVRP:

```
set garp=gvrp port=1-4 mode=none
```

The following command activates GVRP on port 3:

```
set garp=gvrp port=3 mode=normal
```

SET GARP TIMER

Syntax

```
set garp=gvrp timer [default] [jointime=value]
[leavetime=value] [leavealltime=value]
```

Parameters

garp	Specifies the GARP application you want to configure. The only GARP application supported by AT-S63 management software is GVRP.
default	Returns the GARP timers to their default settings.
jointime	Specifies the Join Timer in centiseconds, which are one hundredths of a second. The default is 20 centi seconds. If you change this timer, it must be in relation to the GVRP Leave Timer according to the following equation: Join Timer <= (2 x (GVRP Leave Timer))
leavetimer	Specifies the LeaveTimer in centiseconds, which are one hundredths of a second. The default is 60 centi seconds.
leavealltime	Specifies the LeaveAllTimer in centiseconds. The default is 1000 centiseconds.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command sets the GARP timers.

Note
The settings for these timers must be the same on all GVRP-active network devices.

Examples

The following command sets the Join Period timer to 0.1 second, Leave Period timer to 0.35 seconds, and the LeaveAllPeriod timer to 11 seconds for all GVRP applications:

```
set garp=gvrp timer jointime=10 leavetime=35
leavealltime=1100
```

The following command sets the timers to their default values:

```
set garp=gvrp timer default
```

SHOW GARP

Syntax

```
show garp=gvrp
```

Parameter

garp	Specifies the GARP application you want to display. The only GARP application supported by AT-S63 management software is GVRP.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays current values for the following GARP application parameters:

- GARP application protocol
- GVRP status
- GVRP GIP status
- GVRP Join Time
- GVRP Leave Time
- GVRP Leaveall Time
- Port information
- Mode

Example

The following command displays GVRP information:

```
show garp=gvrp
```

SHOW GARP COUNTER

Syntax

```
show garp=gvrp counter
```

Parameter

garp — Specifies the GARP application you want to display. The only GARP application supported by AT-S63 management software is GVRP.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays the current values for the following GARP packet and message counters:

- GARP application
- Receive: Total GARP Packets
- Transmit: Total GARP Packets
- Receive: Invalid GARP Packets
- Receive Discarded: GARP Disabled
- Receive DIscarded: Port Not Listening
- Transmit Discarded: Port Not Sending
- Receive Discarded: Invalid Port
- Receive Discarded: Invalid Protocol
- Receive Discarded: Invalid Format
- Receive Discarded: Database Full
- Receive GARP Messages: LeaveAll
- Transmit GARP Messages: LeaveAll
- Receive GARP Messages: JoinEmpty
- Transmit GARP Messages: JoinEmpty
- Receive GARP Messages: JoinIn
- Transmit GARP Messages: JoinIn
- Receive GARP Messages: LeaveEmpty
- Transmit GARP Messages: LeaveEmpty

- Receive GARP Messages: LeaveIn
- Transmit GARP Messages: LeaveIn
- Receive GARP Messages: Empty
- Transmit GARP Messages: Empty
- Receive GARP Messages: Bad Message
- Receive GARP Messages: Bad Attribute

Example

The following command displays information for all GARP application counters:

```
show garp=gvrp counter
```

SHOW GARP DATABASE

Syntax

```
show garp=gvrp db|database
```

Parameters

garp — Specifies the GARP application you want to display. The only GARP application supported by AT-S63 management software is GVRP.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays the following parameters for the internal database for the GARP application. Each attribute is represented by a GID index within the GARP application.

- GARP Application
- GID Index
- Attribute
- Used

Example

The following command displays the database for all GARP applications:

```
show garp=gvrp database
```

SHOW GARP GIP

Syntax

```
show garp=gvrp gip
```

Parameter

garp	Specifies the GARP application you want to display. The only GARP application supported by AT-S63 management software is GVRP.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays the following parameters for the GIP-connected ring for the GARP application:

- GARP Application
- GIP contact
- STP ID

Example

The following command displays the GIP-connected ring for all GARP applications:

```
show garp=gvrp gip
```

SHOW GARP MACHINE

Syntax

```
show garp=gvrp machine
```

Parameter

garp — Specifies the GARP application you want to display. The only GARP application supported by AT-S63 management software is GVRP.

> **Note**
> The online help for this command contains an STP option. This option is not supported.

Description

This command displays the following parameters for the GID state machines for the GARP application. The output is shown on a per-GID index basis; each attribute is represented by a GID index within the GARP application.

- VLAN
- Port
- App
- Reg

Example

The following command displays GID state machines for all GARP applications:

```
show garp=gvrp machine
```

Chapter 31

Protected Ports VLAN Commands

This chapter contains the following commands:

- “ADD VLAN GROUP” on page 548
- “CREATE VLAN PORTPROTECTED” on page 550
- “DELETE VLAN” on page 551
- “DESTROY VLAN” on page 553
- “SET VLAN” on page 554
- “SHOW VLAN” on page 555

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 28, “Protected Ports VLANs” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD VLAN GROUP

Syntax 1

```
add vlan=name|vid ports=ports frame=tagged|untagged
group=uplink|1..256
```

Syntax 2

```
add vlan=name|vid [taggedports=ports] [untaggedports=ports]
group=uplink|1..256
```

Parameters

vlan	Specifies the name or VID of the protected ports VLAN where ports are to be added. You can identify the VLAN by either its name or VID.
ports	Specifies the uplink port(s) or the ports of a group. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-22), or both (for example, 1, 5, 14-22). This parameter must be used with the FRAME parameter.
frame	Identifies the new ports as either tagged or untagged. This parameter must be used with the PORTS parameter.
taggedports	Specifies the tagged ports to be added to the VLAN.
untaggedports	Specifies the untagged ports to be added to the VLAN.
group	Specifies that the port(s) being added is an uplink port or belongs to a new group. If the port(s) being added is an uplink port, specify the UPLINK option. Otherwise, specify the group number for the port. The group range is 1 to 256. The number must be unique for each group on the switch.

Description

These commands perform two functions. One is to specify the uplink port of a protected ports VLAN. The other function is to add ports to groups within a VLAN.

Note the following before using this command:

- You must first create the protected ports VLAN by giving it a name and a VID before you can add ports. Creating a VLAN is accomplished with "CREATE VLAN PORTPROTECTED" on page 550.
- Both command syntaxes perform the same function. The difference is that with syntax 1 you can add ports of only one type, tagged or untagged, at a time. With syntax 2, you can add both at the same time.
- If you are adding an untagged port to a group, the port cannot be an untagged member of another protected port VLAN. It must be an untagged member of the Default_VLAN or a port-based or tagged VLAN. To remove a port from a protected port VLAN, use "DELETE VLAN" on page 551.
- You cannot add a new uplink port to a VLAN if the VLAN has already been assigned an uplink port. Instead, you must delete the existing uplink port(s) using the "DELETE VLAN" on page 551 and then re-add the uplink port(s) using this command.
- You cannot add ports to an existing group. To modify an existing group, you must delete the group by removing all ports from it, using "DELETE VLAN" on page 551, and then add the ports back to the group using this command.

Examples

The following command uses Syntax 1 to specify that port 11 is to be an untagged uplink port for the protected ports VLAN called InternetGroups:

```
add vlan=InternetGroups ports=11 frame=untagged group=uplink
```

The following command accomplishes the same thing using Syntax 2:

```
add vlan=InternetGroups untaggedports=11 group=uplink
```

The following command uses Syntax 1 to create group 4 in the InternetGroups VLAN. The group will consist of two untagged ports, 5 and 6:

```
add vlan=InternetGroups port=5,6 frame=untagged group=4
```

The following command does the same thing using Syntax 2:

```
add vlan=InternetGroups untaggedports=5,6 group=4
```

CREATE VLAN PORTPROTECTED

Syntax

```
create vlan=name vid=vid portprotected
```

Parameters

vlan	Specifies the name of the new protected ports VLAN. The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that will be a part of the protected ports VLAN (for example, InternetGroups). The name cannot contain spaces or special characters, such as an asterisk (*) or exclamation point (!).
vid	Specifies a VID for the new protected ports VLAN. The range is 2 to 4094. This number must be unique from the VIDs of all other tagged, untagged, and port protected VLANs on the switch.

Description

This command is the first step to creating a protected ports VLAN. This command assigns a name and VID to the VLAN. The second step is to specify an uplink port and the port groups using “ADD VLAN GROUP” on page 548.

Examples

The following command creates a protected ports VLAN called InternetGroups and assigns it a VID of 12:

```
create vlan=InternetGroups vid=12 portprotected
```

DELETE VLAN

Syntax 1

```
delete vlan=name|vid ports=ports frame=tagged|untagged
```

Syntax 2

```
delete vlan=name|vid [taggedports=ports]
[untaggedports=ports]
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified. You can specify the VLAN by its name or VID.
port	Specifies the port to be removed from the VLAN. You can specify more than one port at a time. This parameter must be used with the FRAME parameter.
frame	Identifies the ports to be removed as tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the tagged ports to be removed from the VLAN.
untaggedports	Specifies the untagged ports to be removed from the VLAN.

Description

This command removes ports from a protected ports VLAN. You can use this command to remove an uplink port or a port from a group.

Note the following before using this command:

- Both command syntaxes perform the same function. The difference is that with Syntax 1 you can delete ports of only one type, tagged or untagged, at a time. With Syntax 2, you can delete both types at the same time.
- Deleting all ports from a group deletes the group from the VLAN.
- Deleted untagged ports are returned to the Default_VLAN as untagged.
- You can delete ports from only one group at a time.

Examples

The following command uses Syntax 1 to delete untagged port 12 from the InternetGroups VLAN:

```
delete vlan=InternetGroups port=12 frame=untagged
```

The following command accomplishes the same thing using Syntax 2:

```
delete vlan=InternetGroups untaggedports=12
```

DESTROY VLAN

Syntax

```
destroy vlan=name|vid|all
```

Parameters

vlan	Specifies the name or VID of the VLAN to be destroyed. To delete all tagged, port-based, and protected ports VLANs on the switch, use the ALL option.

Description

This command deletes VLANs from the switch. You can use this command to delete tagged, port-based, and protected port VLANs. All untagged ports in a deleted VLAN are automatically returned to the Default_VLAN. You cannot delete the Default_VLAN.

Example

The following command deletes the VLAN called InternetGroups:

```
destroy vlan=InternetGroups
```

The following command deletes all VLANs:

```
destroy vlan=all
```

SET VLAN

Syntax

```
set vlan=name|vid port=ports frame=tagged|untagged
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
ports	Specifies the port whose VLAN type is to be changed. You can specify more than one port at a time. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-22), or both (for example, 1, 5, 14-22).
frame	Identifies the new VLAN type for the port. The type can be tagged or untagged.

Description

This command changes a port's VLAN type. You can use this command to change a tagged port to untagged and vice versa.

Before using this command, note the following:

- Changing a port in a port-based, tagged, or protected ports VLAN from untagged to tagged adds the port to the Default_VLAN as untagged.
- Changing a port in the Default_VLAN from untagged to tagged results in the port being an untagged member of no VLAN.
- Changing a port from tagged to untagged removes the port from its current untagged port assignment.

Examples

The following command changes port 4 in the Sales VLAN from tagged to untagged:

```
set vlan=Sales port=4 frame=untagged
```

SHOW VLAN

Syntax

show vlan[=*name*|*vid*]

Parameter

vlan — Specifies the name or VID of the VLAN you want to view. Omitting this displays all VLANs.

Description

This command displays information about the VLANs on the switch. An example of the information displayed by this command for a protected ports VLAN is shown in Figure 53.

```
VLAN Name ............................ Phone_staff_2
VLAN ID .............................. 12
VLAN Type ............................ Protected
Protected Ports ...................... Yes
Uplink Port(s) ....................... 23

Group (ports) ........................ 1(14)
Group (ports) ........................ 2(15)
Group (ports) ........................ 3(16-17)
Group (ports) ........................ 4(18-19)
Group (ports) ........................ 5(20)
Untagged Port(s) ..................... 14-20
Tagged Port(s) ....................... 23
```

Figure 53. SHOW VLAN Command for a Protected Ports VLAN

The information displayed by this command is described here:

- VLAN name - The name of the VLAN.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be Protected for a protected ports VLAN.
- Protected Ports - The status of protected ports. This will be Yes for a protected ports VLANs.
- Uplink Port(s) - The port that is functioning as the unlink port for the groups of the VLAN. There can be more than one uplink port.
- Group (ports) - The group number followed by the ports of the group.
- Untagged port(s) - The untagged ports of the VLAN.
- Tagged port(s) - The tagged ports of the VLAN.

For an example of the information displayed by this command for a port-based or tagged VLAN, see Figure 51 on page 529. For an example of a MAC address-based VLAN, see Figure 54 on page 565.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays the Sales VLAN:

```
show vlan=Sales
```

Chapter 32

MAC Address-based VLAN Commands

This chapter contains the following commands:

- “ADD VLAN MACADDRESS” on page 558
- “ADD VLAN PORT MACADDRESS” on page 559
- “CREATE VLAN TYPE=MACADDRESS” on page 560
- “DELETE VLAN MACADDRESS” on page 562
- “DELETE VLAN PORT MACADDRESS” on page 563
- “DESTROY VLAN” on page 564
- “SHOW VLAN” on page 565

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
MAC address-based VLANs are supported on the AT-9424Ti/SP, AT-9448T/SP, and AT-9448Ts/XP switches. This feature is not supported on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches. For background information, refer to Chapter 29, “MAC Address-based VLANs” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD VLAN MACADDRESS

Syntax

```
add vlan=name|vid macaddress|destaddress=mac-address
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
macaddress ***or*** destaddress	Specifies the MAC address to add to the VLAN. These parameters are equivalent. A MAC address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command adds a MAC address to a MAC address-based VLAN. You can add only one address at a time with this command. The command does not accept ranges or wildcards.

The VLAN must already exist. To create a MAC address-based VLAN, see “CREATE VLAN TYPE=MACADDRESS” on page 560. After you add a MAC address to a VLAN, you can assign it one or more egress ports using “ADD VLAN PORT MACADDRESS” on page 559.

Examples

The following command adds the MAC address 00:30:84:32:8A:5D to the Sales VLAN:

```
add vlan=sales macaddress=00:30:84:32:8a:5d
```

The following command adds the MAC address 00:30:84:32:76:1A to the VLAN with the VID 12:

```
add vlan=12 macaddress=00308432761a
```

ADD VLAN PORT MACADDRESS

Syntax

`add vlan=`*`name`*`|`*`vid`* `port=`*`ports`* `macaddress|destaddress=`*`mac-address`*

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
port	Specifies the egress port(s) to assign to the MAC address. You can specify more than one egress port.
macaddress ***or*** destaddress	Specifies the MAC address to be assigned the egress port(s). The MAC address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command assigns egress ports to a MAC address in a MAC address-based VLAN. The MAC address must already be in the VLAN before you can assign it egress ports. To assign a MAC address to a VLAN, refer to "ADD VLAN MACADDRESS" on page 558.

Examples

The following command assigns ports 1 and 4 as egress ports for the MAC address 00:30:84:32:8A:5D in the Sales VLAN:

```
add vlan=sales port=1,4 macaddress=00:30:84:32:8a:5d
```

The following command assigns port 11 to 14 as egress ports for the MAC address 00:30:84:75:11:B2 from the VLAN with the VID 24:

```
add vlan=24 port=11-14 macaddress=00:30:84:75:11:b2
```

CREATE VLAN TYPE=MACADDRESS

Syntax

```
create vlan=name vid=vid type=macaddress
```

Parameters

vlan	Specifies the name of the VLAN. You must assign a name to a VLAN. The name can be from 1 to 20 characters in length and should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). The name cannot be the same as the name of an existing VLAN on the switch. If the VLAN is unique in your network, then the name needs to be unique as well. If the VLAN spans multiple switches, then the name for the VLAN should be the same on each switch.
vid	Specifies the VLAN identifier. The range is 2 to 4094. The VLAN must be assigned a VID. You cannot use the VID 1, which is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch. If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, assign the Sales VLAN on each switch the same VID value.
type	Specifies the type of VLAN. To create a MAC address-based VLAN, the type must be MACADDRESS.

Description

This command is the first in the series to creating a MAC address-based VLAN. This command assigns the VLAN a name and a VID and sets the VLAN type. After you have initially created the VLAN with this command, you must assign the MAC addresses. These are the source addresses of the nodes that are to belong to the VLAN. The command for adding MAC addresses to a VLAN is "ADD VLAN MACADDRESS" on page 558.

The final step to creating a new MAC address-based VLAN is assigning the egress ports to the MAC addresses. The command for this is "ADD VLAN PORT MACADDRESS" on page 559.

Examples

The following command creates a MAC address-based VLAN called Sales and assigns it a VID of 3:

```
create vlan=Sales vid=3 type=macaddress
```

DELETE VLAN MACADDRESS

Syntax

```
delete vlan=name|vid macaddress|destaddress=mac-address
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
macaddress ***or*** destaddress	Specifies the MAC address to be removed from the VLAN. These parameters are equivalent. You can remove only one MAC address at a time. A MAC address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command removes MAC addresses from a MAC address-based VLAN. You can remove only one MAC address at a time with this command.

You cannot remove a MAC address if it has been assigned egress ports. You must first remove the ports from the MAC address before you can delete it. To remove egress ports from a MAC address, refer to “DELETE VLAN PORT MACADDRESS” on page 563.

Examples

The following command removes the MAC address 00:30:84:32:8A:5D from the Sales VLAN:

```
delete vlan=Sales macaddress=00:30:84:32:8A:5D
```

The following command removes the MAC address 00:30:84:75:11:B2 from the VLAN with the VID 24:

```
delete vlan=24 macaddress=0030847511b2
```

DELETE VLAN PORT MACADDRESS

Syntax

```
delete vlan=name|vid port=ports macaddress=mac-address
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
port	Specifies the egress port to be removed for the MAC address. You can remove more than one egress port at a time.
macaddress	Specifies a MAC address to which the port is assigned. A MAC address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command removes egress ports from a MAC address of a MAC address-based VLAN. You might remove an egress port from a MAC address-based VLAN if you no longer want it to be a part of the VLAN.

Examples

The following command removes port 4 from the MAC address 00:30:84:32:8A:5D in the Sales VLAN:

```
delete vlan=Sales port=4 macaddress=00:30:84:32:8A:5D
```

The following command removes ports 11 to 14 from the MAC address 00:30:84:75:11:B2 in the VLAN with the VID 24:

```
delete vlan=24 port=11-14 macaddress=0030847511b2
```

DESTROY VLAN

Syntax

```
destroy vlan vlan=name|all [vid=vid]
```

Parameters

vlan	Specifies the name of the VLAN to be deleted. To delete all VLANs, use the ALL option.
vid	Specifies the VID of the VLAN to be deleted. This parameter is optional.

Description

The command deletes port-based, tagged, and MAC address-based VLANs. You can use the command to deleted selected VLANS or to delete all VLANs, with the exception of the Default_VLAN.

Examples

The following command deletes the Sales VLAN from the switch:

```
destroy vlan vlan=Sales
```

The following command deletes the Sales VLAN using both the name and the VID:

```
destroy vlan vlan=Sales vid=102
```

The following command deletes all port-based and tagged VLANs on a switch:

```
destroy vlan=all
```

SHOW VLAN

Syntax

show vlan[=*name*|*vid*]

Parameter

vlan Specifies the name or VID of the VLAN.

Description

This command displays the VLANs on the switch. An example of the information displayed by this command for a MAC address-based VLAN is shown in Figure 54.

```
VLAN Name ............................ Sales
VLAN ID .............................. 4
VLAN Type ............................ MAC Based
Protected Ports ...................... No
Untagged Port(s) ..................... None
Tagged Port(s) ....................... None
MAC Associations:
  Total number of associated MAC addresses: 5
  ------------------------------------------------
  MAC Address            Ports
  ------------------------------------------------
  00:06:5B:44:44:44      4-8
  00:06:5B:55:55:55      4
  00:06:5B:66:66:66      4
  00:06:5B:77:77:77      4
  00:06:5B:88:88:88      4
  ------------------------------------------------
```

Figure 54. SHOW VLAN Command for a MAC Address-based VLAN

The information displayed by the command is described here:

- VLAN name - The name of the VLAN.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be MAC Based for a MAC address-based VLAN.
- Protected Ports - The status of protected ports. This will be No for a MAC address-based VLAN.
- Untagged port(s) - The untagged ports of the VLAN. This will be None for a MAC address-based VLAN.
- Tagged port(s) - The tagged ports of the VLAN. This will be None for a MAC address-based VLAN.

- MAC Address / Ports - The MAC addresses of the VLAN and the egress ports.

For an example of the information displayed by this command for a port-based or tagged VLAN, see Figure 51 on page 529. For an example of a protected ports VLAN, see Figure 53 on page 555.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays information on only the Sales VLAN:

```
show vlan=sales
```

The following command displays information the VLAN with the VID of 22:

```
show vlan=22
```

Section VII

Port Security

The chapters in this section provide the commands for configuring port security using the AT-S63 management software. The chapters include:

- Chapter 33, “MAC Address-based Port Security Commands” on page 569
- Chapter 34, “802.1x Port-based Network Access Control Commands” on page 577

Chapter 33

MAC Address-based Port Security Commands

This chapter contains the following command:

- "SET SWITCH PORT INTRUSIONACTION" on page 570
- "SET SWITCH PORT SECURITYMODE" on page 571
- "SHOW SWITCH PORT INTRUSION" on page 574
- "SHOW SWITCH PORT SECURITYMODE" on page 575

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 30, "MAC Address-based Port Security" in the *AT-S63 Management Software Menus Interface User's Guide*.

SET SWITCH PORT INTRUSIONACTION

Syntax

```
set switch port=port intrusionaction=discard|trap|disable
```

Parameters

port — Specifies the port where you want to change the intrusion action. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

intrusionaction — Specifies the action the port takes when it receives an invalid frame. The options are:

- discard — The port discards invalid frames. This is the default.
- trap — The port discards invalid frames and sends an SNMP trap.
- disable — The port discards invalid frames, sends an SNMP trap, and disables the port.

Description

This command defines what a port does when it receives an invalid frame. and applies only to ports operating in the Limited security mode.

Example

The following command sets the intrusion action to trap on ports 12 and 21:

```
set switch port=12,21 intrusionaction=trap
```

SET SWITCH PORT SECURITYMODE

Syntax

```
set switch port=port
[securitymode=automatic|limited|secured|locked]
[intrusionaction=discard|trap|disable]
[learn=value] [participate=yes|no|on|off|true|false]
```

Parameters

port — Specifies the port where you want to set security. You can specify more than one port at a time.You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

securitymode — Specifies the port's security mode. Options are:

- automatic — Disables security on the port. This is the default setting.
- limited — Sets the port to the Limited security mode. The port learns a limited number of dynamic MAC addresses, set with the LEARN parameter.
- secured — Sets the port to the Secured security mode. The port accepts frames based only on static MAC addresses. You must enter the static MAC addresses of the nodes with frames the port is to accept after you have activated this security mode on a port. To add static MAC addresses, use the command "ADD SWITCH FDB|FILTER" on page 156.
- locked — Sets the switch to the Locked security mode. The port stops learning new dynamic MAC addresses. The port forwards frames based on static MAC addresses and on those dynamic addresses it has already learned.

Note
The online help for this command includes a "pacontrol" option for this parameter. The option is nonfunctional.

intrusionaction — Specifies the action taken by the port in the event port security is violated. This parameter applies only to the Limited security mode. Intrusion actions are:

- discard — Discards invalid frames. This is the default setting.
- trap — Discards invalid frames and sends a management trap.
- disable — Discards invalid frames, sends a management trap, and disables the port.

The intrusion action of a port operating in the Secured or Locked security level is to discard invalid frames.

learn — Specifies the maximum number of dynamic MAC addresses a port on the switch can learn. This parameter applies only to ports set to the Limited security mode. The range is 1 to 255 addresses. The default is 255.

participate — Enables or disables the intrusion action on the port. This option only applies to the Limited security mode and only when a port's intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard. The options are:

- yes, on, true — Enables the trap or disable intrusion action. These options are equivalent.
- no, off, false — Disables the trap or disable intrusion action. The port still discards invalid ingress frames. This is the default. These options are equivalent.

Description

This command sets and configures a port's security mode. Only one mode can be active on a port at a time.

Note
For explanations of the security levels and intrusion actions, refer to Chapter 30, "MAC Address Port Security" in the *AT-S63 Management Software Menus Interface User's Guide*.

To view a port's current security mode, use the command "SHOW SWITCH PORT SECURITYMODE" on page 575.

The management software displays a confirmation prompt whenever you perform this command. Responding with **Y** for yes completes your command, while **N** for no cancels the command.

Examples

The following command sets the security level for port 8 to the Limited mode and specifies a limit of 5 dynamic MAC addresses. Because no intrusion action is specified, the discard action is assigned by default:

```
set switch port=8 securitymode=limited learn=5
```

The following command sets the security level for ports 9 and 12 to the Limited mode and specifies a limit of 15 dynamic MAC addresses per port. The disable intrusion action is specified:

```
set switch port=9,12 securitymode=limited learn=15
intrusionaction=disable participate=yes
```

In the above example, the Participate option is required to activate the disable intrusion action. Without it, the port would discard invalid ingress frames but would not send an SNMP trap and disable the port.

The following command changes the maximum number of learned MAC addresses to 150 on ports 15 and 16. The command assumes that the ports have already be set to the Limited security mode:

```
set switch port=15-16 learn=150
```

The following command sets the security level to Locked for ports 2, 6, and 18:

```
set switch port=2,6,18 securitymode=locked
```

The Limit and Participate options are not included with the above command because they do not apply to the Locked mode, nor to the Secured mode.

The following command sets the security level to Secured for ports 12 to 24:

```
set switch port=12-24 securitymode=secured
```

The following command returns ports 8 to 11 to the automatic security level, which disables port security:

```
set switch port=8-11 securitymode=automatic
```

SHOW SWITCH PORT INTRUSION

Syntax

```
show switch port=port intrusion
```

Parameter

port	Specifies the port where you want to view the number of intrusions that have occurred. You can specify more than one port at a time.

Description

This command displays the number of times a port has detected an intrusion violation. An intrusion violation varies depending on the security mode:

- Limited Security Level - An intrusion is an ingress frame with a source MAC address not already learned by a port after the port had reached its maximum number of dynamic MAC addresses, or that was not assigned to the port as a static address.
- Secured Security Level - An intrusion is an ingress frame with a source MAC address that was not entered as a static address on the port.
- Locked - An intrusion is an ingress frame with a source MAC address that the port has not already learned or that was not assigned as a static address.

Example

The following command displays the number of intrusion violations detected on ports 12 and 21:

```
set switch port=12,21 intrusion
```

SHOW SWITCH PORT SECURITYMODE

Syntax

```
show switch port=port securitymode
```

Parameters

port	Specifies the port whose security mode settings you want to view. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command displays the security mode settings for the ports on the switch. An example of the information displayed by this command is shown in Figure 55.

```
Port    Security Mode      Intrusion Action    Participating     MAC Limit
-------------------------------------------------------------------------
1       Secured            ----                ----              ----
2       Limited            Trap                Yes               20
3       Limited            Trap                Yes               20
4       Limited            Trap                Yes               20
5       Automatic          ----                ----              ----
6       Automatic          ----                ----              ----
```

Figure 55. SHOW SWITCH PORT SECURITYMODE Command

The columns in the display are defined here:

- Port - Port number.
- Security Mode - The current security mode of the port. Possible settings are Automatic (no security), Limited, Secured, and Locked. For definitions of the security levels, refer to "SET SWITCH PORT SECURITYMODE" on page 571.
- Intrusion Action - The action taken by a port operating with the Limited security level when it detects an intrusion violation.
- Participating - The status of intrusion action on the port. This option only applies to the Limited security mode and only when a port's intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard.
- MAC Limit - The maximum number of dynamic MAC addresses the port can learn. This parameter applies only to the Limited security mode.

Example

The following command displays the security mode settings for ports 1 to 5:

```
show switch port=1-5 securitymode
```

Chapter 34

802.1x Port-based Network Access Control Commands

This chapter contains the following commands:

- “DISABLE PORTACCESS|PORTAUTH” on page 578
- “DISABLE RADIUSACCOUNTING” on page 579
- “ENABLE PORTACCESS|PORTAUTH” on page 580
- “ENABLE RADIUSACCOUNTING” on page 581
- “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 582
- “SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT” on page 590
- “SET RADIUSACCOUNTING” on page 592
- “SHOW PORTACCESS|PORTAUTH” on page 594
- “SHOW PORTACCESS|PORTAUTH PORT” on page 596
- “SHOW RADIUSACCOUNTING” on page 599

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 31, “802.1x Port-based Network Access Control” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE PORTACCESS|PORTAUTH

Syntax

```
disable portaccess|portauth
```

> **Note**
> The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

None.

Description

This command disables 802.1x Port-based Network Access Control on the switch. This is the default setting.

Example

The following command disables 802.1x Port-based Network Access Control on the switch:

```
disable portaccess
```

DISABLE RADIUSACCOUNTING

Syntax

```
disable radiusaccounting
```

Parameters

None

Description

This command disables RADIUS accounting on the switch.

Example

The following command disables RADIUS accounting:

```
disable radiusaccounting
```

Equivalent Command

```
set radiusaccounting status=disabled
```

For information, see "SET RADIUSACCOUNTING" on page 592.

ENABLE PORTACCESS|PORTAUTH

Syntax

```
enable portaccess|portauth
```

> **Note**
> The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

None.

Description

This command activates 802.1x Port-based Network Access Control on the switch. The default setting for this feature is disabled.

> **Note**
> You should activate and configure the RADIUS client software on the switch before activating port-based access control. Refer to “SET AUTHENTICATION” on page 658.

Example

The following command activates 802.1x Port-based Network Access Control on the switch:

```
enable portaccess
```

ENABLE RADIUSACCOUNTING

Syntax

```
enable radiusaccounting
```

Parameters

None

Description

This command activates RADIUS accounting on the switch.

Example

The following command activates RADIUS accounting:

```
enable radiusaccounting
```

Equivalent Command

```
set radiusaccounting status=enabled
```

For information, see "SET RADIUSACCOUNTING" on page 592.

SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR

Syntax

```
set portaccess|portauth=8021x|macbased port=port
type|role=authenticator|none [mode=single|multiple]
[control=auto|authorised|forceauthenticate|
unauthorised|forceunauthenticate]
[quietperiod=value] [txperiod=value]
[reauthenabled=enabled|disabled] [reauthperiod=value]
[supptimeout=value] [servertimeout|servtimeout=value]
[maxreq=value] [ctrldirboth=ingress|both]
[piggyback=enabled|disabled] [guestvlan=vlan-name|vid|none]
[vlanassignment=enabled|disabled] [securevlan=on|off]
```

Parameters

portaccess **or** portauth	Specifies the authentication method. The two choices are:	
	8021x	Specifies 802.1x username and password authentication. With this authentication method the supplicant must provide, either manually or automatically, a username and password. This authentication method requires 802.1x client software on the supplicant nodes.
	macbased	Specifies MAC address-based authentication. The authenticator port extracts the source MAC address from the initial frames received from a supplicant and automatically sends the address as both the username and password of the supplicant to the authentication server. This authentication method does not require 802.1x client software on the supplicant nodes.
port	Specifies the port to set to the Authenticator role or whose Authenticator settings you want to adjust. You can specify more than one port at a time.	

type ***or*** role	Specifies the role of the port. The parameters are equivalent. The options are:	
	authenticator	Specifies the authenticator role.
	none	Disables port-based access control on the port.
mode	Controls the operating mode of an authenticator port. The options are:	
	single	Configures the port to accept only one authentication. This authenticator mode should be used together with the piggy-back mode. When an authenticator port is set to the single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port. This is the default setting.
	multi	Configures the port to accept up to 20 authentications. Every client using an authenticator port in this mode must have a username and password combination and log on separately.
control	Specifies the authenticator state. The options are:	
	auto	Sets the port state to 802.1X port-based authentication. The port begins in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes. The switch requests the identity of the client and begins relaying authentication messages between the client

		and the authentication server. Each client that attempts to access the network is uniquely identified by the switch by using the client's MAC address. This is the default setting.
	authorised ***or*** forceauthenticate	Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The parameters are equivalent.
	unauthorised ***or*** forceunauthenticate	Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. The parameters are equivalent.
quietperiod	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.	
txperiod	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.	
reauthenabled	Controls whether the client must periodically reauthenticate. The options are:	
	enabled	Specifies that the client must periodically reauthenticate. This is the default setting. The time period between reauthentications is set with the reauthperiod parameter.
	disabled	Specifies that reauthentication by the client is not required after the initial authentication. Reauthentication is only required if there is a change to the status

of the link between the supplicant and the switch or the switch is reset or power cycled.

reauthperiod — Enables periodic reauthentication of the client, which is disabled by default. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

supptimeout — Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

servertimeout ***or*** servtimeout — Sets the timer used by the switch to determine authentication server timeout conditions. The default value is 10 seconds. The range is 1 to 60 seconds. The parameters are equivalent.

maxreq — Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The range is 1 to 10 retransmissions and the default is 2.

ctrldirboth — Specifies how the port is to handle ingress and egress broadcast and multicast packets when in the unauthorized state. \

When a port is set to the authenticator role, it remains in the unauthorized state until a client is authenticated by the authentication server. In the unauthorized state, the port accepts only EAP packets from the client. All other ingress packets the port might receive from the supplicant, including multicast and broadcast traffic, are discarded until the supplicant has been authenticated.

You can use this selection to control how an authenticator port handles egress broadcast and multicast traffic when in the unauthorized state. You can instruct the port to forward this traffic to the client, even though the client has not logged on, or you can have the port discard the traffic.

The options are:

ingress — An authenticator port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client while forwarding all egress broadcast and multicast traffic to the same client. This is the default setting.

both — An authenticator port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the client until the client has logged on.

This parameter is only available when the authenticator's operating mode is set to single. When set to multiple, an authenticator port does not forward ingress or egress broadcast or multicast packets until at least one client has logged on.

piggyback — Controls who can use the switch port in cases where there are multiple clients using the port, for example the port is connected to an Ethernet hub. This parameter is applicable when the authenticator's operating mode is set to single. The options are:

- enabled — Allows all clients on the port to piggy-back onto the initial client's authentication, causing the port to forward all packets after one client is authenticated. This is the default setting.
- disabled — Specifies that the switch port forward only those packets from the client who is authenticated and discard packets from all other users.

guestvlan — Specifies the name or VID of a Guest VLAN. The authenticator port is a member of a Guest VLAN when no supplicant is logged on. Clients do not log on to access a Guest VLAN.

If an authenticator port where a Guest VLAN has been defined starts to receive EAPOL packets, signalling that a supplicant is logging on, it changes to the unauthorized state and moves from the Guest VLAN to its predefined VLAN. The port remains in the unauthorized state until the log on process between the supplicant and the RADIUS server is completed.

The options are:

- vlan-name — Specifies the name of the Guest VLAN.
- vlan-id — Specifies the VID of the Guest VLAN.
- none — Removes a predefined Guest VLAN from an authenticator port.

A Guest VLAN is only supported when the operating mode of the port is set to Single. The specified VLAN must already exit on the switch.

vlanassignment — Specifies whether to use the VLAN assignments entered in the user accounts on the RADIUS server. Options are:

- enabled — Specifies that the authenticator port is to use the VLAN assignments returned by the RADIUS server when a supplicant logs on. This is the default setting.
- disabled — Specifies that the authenticator port ignore any VLAN assignment information returned by the RADIUS server when a supplicant logs on. The authenticator port remains in its predefined VLAN assignment even when the RADIUS server returns a VLAN assignment when a supplicant logs on.

securevlan — Controls the action of an authenticator port to subsequent authentications after the initial authentication where VLAN assignments have been added to the user accounts on the RADIUS server. This parameter only applies when the port is operating in the Multiple operating mode.

- on — Specifies that only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with a different or no VLAN assignment are denied entry to the port. This is the default setting.
- off — Specifies that all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication, regardless of the VLAN assignments of subsequent authentications.

Description

This command sets ports to the authenticator role and configures the authenticator role parameters. This command also disables port-based access control on a port.

Examples

The following command sets ports 4 to 6 to the authenticator role. The authentication method is set to 802.1x, meaning that the supplicants must have 802.1x client software and provide a username and password, either automatically or manually, when logging on and during reauthentications. The operating mode is set to Single and the piggy back mode to disabled. At these settings, only one supplicant can use each port. After a supplicant logs on, access by any other client to the same port is denied:

```
set portaccess=8021x port=4-6 role=authenticator mode=single
piggyback=disabled
```

The next command is identical to the previous example, except the authentication method is MAC address-based, meaning the authenticator ports use the MAC addresses of the supplicants as the usernames and passwords. With MAC address-based authentication, an authenticator port automatically extracts the MAC address from the initial frames received from a supplicant and sends it to the RADIUS server. The supplicants do not need 802.1x client software. Again, as in the previous example, since the operating mode is Single and the piggy back mode is disabled only one supplicant can use each port.

```
set portaccess=macbased port=4-6 role=authenticator
mode=single piggyback=disabled
```

Note
The remaining examples are limited to the 802.1x authentication method, but apply equally to the MAC address-based authentication method.

The following command sets port 12 to the authenticator role and the operating mode to Single. The difference between this and the previous example is the piggy back mode is enabled. This configuration is appropriate when an authenticator port is supporting multiple clients, such as when a port is connected to an Ethernet hub, and you do not want to give each supplicant a separate username and password combination on the RADIUS server. With the piggy back mode enabled, all of the clients connected to the port can access it after one supplicant logs on:

```
set portaccess=8021x port=12 role=authenticator mode=single
piggyback=enabled
```

The following command sets port 22 to the authenticator role and the operating mode to Multiple. This configuration is also appropriate where there is more than one supplicant on a port. But an authenticator port in the Multiple mode requires that all supplicants have their own username and password combinations on the RADIUS server and that they log on before they can use the authenticator port on the switch:

```
set portaccess=8021x port=22 role=authenticator mode=multi
```

The following command assigns the Guest VLAN "Product_show" to authenticator ports 5 and 12. The ports function as untagged members of the VLAN and allow any network user access to the VLAN without logging on. However, should a port start to receive EAPOL packets, it assumes that a supplicant is initiating a log on and changes to the unauthorized state. After the log on is completed, the port moves to its predefined VLAN:

```
set portaccess=8021x port=5,12 role=authenticator
guestvlan=product_show
```

The following command configures port 15 as an authenticator port. This example assumes that the user accounts on the RADIUS server have VLAN assignments. With the VLANASSIGNMENT parameter set to enabled, the port processes the VLAN assignments it receives from the RADIUS server. Had this parameter been disabled, the port would ignore the VLAN assignments and leave the port in its predefined VLAN assignment. The VLAN assignment of the port is determined by the initial log on by a client. With the SECUREVLAN parameter set to enabled, only those subsequent supplicants having the same VLAN assignment as the initial supplicant are allowed to use the port:

```
set portaccess=8021x port=15 role=authenticator
mode=multiple vlanassignment=enabled securevlan=enabled
```

The following command sets port 7 to the authenticator role, the quiet period on the port to 30 seconds, and the server timeout period to 200 seconds:

```
set portaccess=8021x port=7 role=authenticator
quietperiod=30 servtimeout=200
```

The following command configures authenticator port 5 to the multiple operating mode:

```
set portaccess=8021x port=5 role=authenticator mode=multi
```

The following command configures authenticator port 5 to the single operating mode and disables piggy backing:

```
set portaccess=8021x port=5 role=authenticator mode=single
piggyback=disabled
```

The following command disables port-based access control on ports 12 and 15:

```
set portaccess=8021x port=12,15 role=none
```

SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT

Syntax

```
set portaccess|portauth port=port type|role=supplicant|none
[authperiod=value] [heldperiod=value] [maxstart=value]
[startperiod=value] [username|name=name]
[password=password]
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

port — Specifies the port that you want to set to the supplicant role or whose supplicant settings you want to adjust. You can specify more than one port at a time.

type ***or*** role — Specifies the role of the port. The parameters are equivalent. The options are:

- supplicant — Specifies the supplicant role.
- none — Disables port-based access control on the port.

authperiod — Specifies the period of time in seconds that the supplicant will wait for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 60 seconds. The default is 30 seconds.

heldperiod — Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535. The default value is 60.

maxstart — Specifies the maximum number of times the supplicant will send EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

startperiod — Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.

username ***or*** name	Specifies the username for the switch port. The parameters are equivalent. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case-sensitive.
password	Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case-sensitive.

Description

This command sets ports to the supplicant role and configures the supplicant role parameters. This command also disables port-based access control on the port.

Examples

The following command sets ports 4 to 6 to the supplicant role:

```
set portacess port=4-6 role=supplicant
```

The following command sets port 8 to the supplicant role, the name to "switch22," and the password to "bluebird":

```
set portaccess port=8 role=supplicant name=switch22
password=bluebird
```

The following command disables port-based access control on ports 12 and 15:

```
set portaccess port=12,15 role=none
```

SET RADIUSACCOUNTING

Syntax

```
set radiusaccounting [status=enabled|disabled]
[serverport=value] [type=network]
[trigger=start_stop|stop_only]
[updateenable=enabled|disabled] [interval=value]
```

Parameters

status — Activates and deactivates RADIUS accounting on the switch. The options are:

- enabled — Activates RADIUS accounting. This option is equivalent to “ENABLE RADIUSACCOUNTING” on page 581.
- disabled — Deactivates the feature. This is the default. This option is equivalent to “DISABLE RADIUSACCOUNTING” on page 579.

serverport — Specifies the UDP port for RADIUS accounting. The default is port 1813.

type — Specifies the type of RADIUS accounting. The default is Network. This value cannot be changed.

trigger — Specifies the action that causes the switch to send accounting information to the RADIUS server. The options are:

- start_stop — The switch sends accounting information whenever a client logs on or logs off the network. This is the default.
- stop_only — The switch sends accounting information only when a client logs off.

updateenable — Specifies whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled. If you enable this feature, use the INTERVAL parameter to specify the intervals at which the switch is to send the accounting updates.

interval — Specifies the intervals at which the switch is to send interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

Description

RADIUS accounting is supported on those switch ports operating in the Authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. This feature is disabled by default on the switch.

Examples

The following command activates RADIUS accounting and sets the trigger to stop only:

```
set radiusaccounting status=enabled trigger=stop_only
```

The following command enables the update feature and sets the interval period to 200 seconds:

```
set radiusaccounting updateenable=enabled interval=200
```

SHOW PORTACCESS|PORTAUTH

Syntax

```
show portaccess|portauth=8021x|macbased
```

Parameters

portaccess **or** portauth	Specifies the authenticator method of the port. Options are:	
	8021x	Displays information for an 802.1x authenticator port.
	macbased	Displays information for a MAC address-based authenticator port.
config	Displays whether port-based access control is enabled or disabled on the switch.	
status	Displays the role and status of each port.	

Description

This command displays the port roles. Figure 56 is an example of the information displayed by this command.

```
802.1x Authentication Information
-------------------------------------------------
SystemAuthControl.................. Disabled
Number of 802.1x Supplicants....... 0 (480)

Port  Role           Supplicant    Protocol
                     Mode          Version
-------------------------------------------------
1     Authenticator  Single        1
2     Authenticator  Single        1
3     Authenticator  Single        1
4     Authenticator  Single        1
5     Authenticator  Single        1
6     Authenticator  Single        1
7     Authenticator  Single        1
8     Authenticator  Single        1
```

Figure 56. SHOW PORTACCESS|PORTAUTH Command

Examples

The following command displays the port roles of all the ports.

```
show portaccess
```

The following command displays just the 802.1x authenticator ports:

```
show portaccess=8021x
```

The following command displays just the MAC address-based authenticator ports:

```
show portaccess=macbased
```

SHOW PORTACCESS|PORTAUTH PORT

Syntax

```
show portaccess|portauth=8021x|macbased port=port
authenticator|supplicant [config] [status]
```

Parameters

portaccess **or** portauth	Specifies the authenticator method of the port. Options are: 8021x — Displays information for an 802.1x authenticator port. macbased — Displays information for a MAC address-based authenticator port.
port	Specifies the port whose port-based access control settings you want to view. You can specify more than one port at a time.
authenticator	Indicates that the port is an authenticator.
supplicant	Indicates that the port is a supplicant.
config	Displays the port-based access control settings for the port. Omitting this option and the STATUS option displays information on both.
status	Displays the status and role of the port. Omitting this option and the CONFIG option displays information on both.

Description

This command displays information about authenticator and supplicant ports.

Figure 57 illustrates the information displayed by this command for a authenticator port. For an explanation of the parameters, refer to “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 582.

```
Port 1

PAE Type.................. Authenticator
Supplicant Mode........... Single
AuthControlPortControl.... Auto
quietPeriod............... 60
txPeriod.................. 30
suppTimeout............... 30
serverTimeout............. 30
maxReq.................... 2
reAuthPeriod.............. 3600
reAuthEnabled............. Enabled
vlanAssignment............ Enabled
secureVlan................ On
guestVlan................. None (VID=0)
adminControlDirection..... Both
piggyBack................. Disabled

Attached Supplicant(s)
MAC Address..................... -
   Authenticator PAE State......... Connecting
   Port Status..................... Unauthorized
   Backend Authenticator State..... Initialize
```

Figure 57. Authenticator Port Information

Figure 58 illustrates the information displayed for a supplicant port. For an explanation of the parameters, refer to "SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT" on page 590.

```
Port 5

PAE Type.................. Supplicant
heldPeriod...................... 60
authPeriod...................... 30
startPeriod..................... 30
maxStart........................ 3
Supplicant PAE State............ Connecting
```

Figure 58. Supplicant Port Information

Examples

The following command displays the configuration and status for port 10, which is an 802.1x authenticator port:

```
show portaccess=8021x port=10 authenticator
```

The following command displays the configuration and status for port 12 which is a MAC address-based authenticator port:

```
show portaccess=8021x=macbased port=12 authenticator
```

This command displays the port access configuration of port 17, which is a supplicant port:

```
show portaccess port=17 supplicant
```

SHOW RADIUSACCOUNTING

Syntax

```
show radiusaccounting
```

Parameters

None.

Description

This command displays the current parameter settings for RADIUS accounting, which sends updates of supplicant activity on the switch's authenticator ports to the RADIUS server. Figure 59 is an example of the information displayed by this command.

```
Radius Accounting Configuration
-----------------------------------
Radius Accounting Status ...........: Enabled
Radius Accounting Port..............: 1813
Radius Accounting Type..............: Network
Radius Accounting Trigger Type......: Start_Stop
Radius Accounting Update Status.....: Disabled
Radius Accounting Update Interval...: 60
```

Figure 59. SHOW RADIUSACCOUNTING Command

The information displayed by this command is described here:

- Radius Accounting Status - Specifies the status of RADIUS accounting on the switch. A status of Enabled means that the switch is sending supplicant updates to the RADIUS server: A status of Disabled means that the feature is not activated. The default is disabled.
- Radius Accounting Port - Specifies the UDP port for RADIUS accounting. The default is port 1813.
- Radius Accounting Type - Specifies the type of RADIUS accounting. The only possible setting is Network.
- Radius Accounting Trigger Type - Specifies the action that causes the switch to send accounting information to the RADIUS server. An action of Start_Stop sends accounting information whenever a client logs on or logs off the network. This is the default. An action of Stop_Only sends accounting information only when a client logs off.
- Radius Accounting Update Status - Specifies whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled.

- Radius Accounting Update Interval - Specifies the interval at which the switch sends interim accounting updates to the RADIUS server. The default is 60 seconds.

Example

The following command displays the current parameter settings for RADIUS accounting:

```
show radiusaccounting
```

Section VIII

Management Security

The chapters in this section contain the commands for configuring management security using the AT-S63 management software. The chapters include:

- Chapter 35, “Web Server Commands” on page 603
- Chapter 36, “Encryption Key Commands” on page 613
- Chapter 37, “Public Key Infrastructure (PKI) Certificate Commands” on page 621
- Chapter 38, “Secure Sockets Layer (SSL) Commands” on page 637
- Chapter 39, “Secure Shell (SSH) Commands” on page 641
- Chapter 40, “TACACS+ and RADIUS Commands” on page 649
- Chapter 41, “Management ACL Commands” on page 661

Chapter 35

Web Server Commands

This chapter contains the following commands:

- “DISABLE HTTP SERVER” on page 604
- “ENABLE HTTP SERVER” on page 605
- “PURGE HTTP SERVER” on page 606
- “SET HTTP SERVER” on page 607
- “SHOW HTTP SERVER” on page 612

Note
Remember to use the SAVE CONFIGURATION command to save your changes.

Note
For background information on this feature, refer to Chapter 32, “Web Server” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE HTTP SERVER

Syntax

```
disable http server
```

Parameters

None.

Description

This command disables the web server on the switch. When the server is disabled, you cannot manage the switch from a web browser. To view the current status of the web server, see “SHOW HTTP SERVER” on page 612. The default setting for the web server is enabled.

Example

The following command disables the web server:

```
disable http server
```

ENABLE HTTP SERVER

Syntax

```
enable http server
```

Parameters

None.

Description

This command activates the web server on the switch. Activating the server allows you to manage the unit from a web browser. To view the current status of the web server, see "SHOW HTTP SERVER" on page 612. The default setting for the web server is enabled.

Example

The following command activates the web server:

```
enable http server
```

PURGE HTTP SERVER

Syntax

```
purge http server
```

Parameters

None.

Description

This command resets the HTTP server to its default values, as specified in Appendix A, “AT-S63 Default Settings” in the *AT-S63 Management Software Menus Interface User’s Guide*. To view the current web server settings, refer to “SHOW HTTP SERVER” on page 612.

Example

The following command resets the web server parameters to their default values:

```
purge http server
```

SET HTTP SERVER

Syntax

```
set http server [security=enabled|disabled] [sslkeyid=key-id] [port=port]
```

Parameters

security — Specifies the security mode of the web server. The options are:

- enabled — Specifies that the web server is to function in the secure HTTPS mode.
- disabled — Specifies that the web server is to function in the non-secure HTTP mode. This is the default.

sslkeyid — Specifies a key pair ID. This parameter is required if you are configuring the web server to operate in the secure HTTPS mode.

port — Specifies the TCP port number that the web server will listen on. The default for non-secure HTTP operation is port 80. The default for secure HTTPS operation is port 443.

Description

This command configures the web server. You can configure the server for either secure HTTPS or non-secure HTTP operation.

Before configuring the web server, please note the following:

- You cannot use this command when the web server is enabled. You must first disable the web server before making changes. To disable the server, refer to "DISABLE HTTP SERVER" on page 604.
- To configure the web server for the HTTPS secure mode, you must first create an encryption key and a certificate, and add the certificate to the certificate database. The management software will not allow you to configure the web server for the secure HTTPS mode until those steps have been completed.

Examples

The following command configures the web server for the non-secure HTTP mode. Since no port is specified, the default HTTP port 80 is used:

```
set http server security=disabled
```

The following command configures the web server for the secure HTTPS mode. It specifies the key pair ID as 5. Since no port is specified, the default HTTPS port 443 is used:

```
set http server security=enabled sslkeyid=5
```

General Configuration Steps for a Self-signed Certificate

Below are the steps to configuring the switch's web server for a self-signed certificate using the command line commands:

1. Set the switch's date and time. You can do this manually using "SET DATE" on page 95 or you can configure the switch to obtain the date and time from an SNTP server using "ADD SNTPSERVER PEER|IPADDRESS" on page 90.
2. Create an encryption key pair using "CREATE ENCO KEY" on page 614 (syntax 1).
3. Create the self-signed certificate using "CREATE PKI CERTIFICATE" on page 624.
4. Add the self-signed certificate to the certificate database using "ADD PKI CERTIFICATE" on page 622.
5. Disable the switch's web server using "DISABLE HTTP SERVER" on page 604.
6. Configure the web server using "SET HTTP SERVER" on page 607.
7. Activate the web server using "ENABLE HTTP SERVER" on page 605.

The following is an example of the command sequence to configuring the web server for a self-signed certificate. (The example does not include step 1, setting the system time.)

1. This command creates the encryption key pair with an ID of 4, a length of 512 bits, and the description "Switch 12 key":

   ```
   create enco key=4 type=rsa length=512 description="Switch
   12 key"
   ```

2. This command creates a self-signed certificate using the key created in step 1. The certificate is assigned the filename "Sw12cert.cer. (The ".cer" extension is not included in the command because it is added automatically by the management software.) The certificate is assigned the serial number 0 and a distinguished name of 149.11.11.11, which is the IP address of a master switch:

   ```
   create pki certificate=Sw12cert keypair=4 serialnumber=0
   subject="cn=149.11.11.11"
   ```

3. This command adds the new certificate to the certificate database. The certificate is given a description of "Switch 12 certificate":

   ```
   add pki certificate="Switch 12 certificate"
   location=Sw12cert.cer
   ```

4. This command disables the web server:

   ```
   disable http server
   ```

5. This command configures the web server by activating HTTPS and specifying the encryption key pair created in step 1:

   ```
   set http server security=enabled sslkeyid=4
   ```

6. This command enables the web server:

   ```
   enable http server
   ```

General Configuration Steps for a CA Certificate

Below are the steps to configuring the switch's web server for CA certificates using the command line commands. The steps explain how to create an encryption key and a self-signed certificate, and how to configure the web server for the certificate:

1. Set the switch's date and time. You can do this manually using the "SET DATE" on page 95 or you can configure the switch to obtain the date and time from an SNTP server using "ADD SNTPSERVER PEER|IPADDRESS" on page 90.

2. Create an encryption key pair using "CREATE ENCO KEY" on page 614 (syntax 1).

3. Set the switch's distinguished name using "SET SYSTEM DISTINGUISHEDNAME" on page 634.

4. Create an enrollment request using "CREATE PKI ENROLLMENTREQUEST" on page 627.

5. Upload the enrollment request from the switch to a management station or FTP server using “UPLOAD METHOD=XMODEM” on page 246 or “UPLOAD METHOD=TFTP” on page 243.

6. Submit the enrollment request to a CA.

7. After you have received the CA certificates, download them into the switch’s file system using “LOAD METHOD=XMODEM” on page 232 or “LOAD METHOD=TFTP” on page 228.

8. Add the CA certificates to the certificate database using “ADD PKI CERTIFICATE” on page 622.

9. Disable the switch’s web server using the command “DISABLE HTTP SERVER” on page 604.

10. Configure the web server using “SET HTTP SERVER” on page 607.

11. Activate the web server using “ENABLE HTTP SERVER” on page 605

The following is an example of the command sequence for configuring the web server for CA certificates. It explains how to create an encryption key and enrollment request, and how to download the CA certificates on the switch. (The example does not include step 1, setting the system time, and the procedure for submitting the request to a CA, which will vary depending on the enrollment requirements of the CA.)

1. This command creates the encryption key pair with an ID of 8, a length of 512 bits, and the description “Switch 24 key”:

   ```
   create enco key=8 type=rsa length=512 description="Switch
   24 key"
   ```

2. This command sets the switch’s distinguished name to the IP address 149.44.44.44, which is the IP address of a master switch:

   ```
   set system distinguishedname="cn=149.44.44.44"
   ```

3. This command creates an enrollment request using the encryption key created in step 1. It assigns the request the filename “sw24cer.csr”. The command omits the “.csr” extension because the management software adds it automatically:

   ```
   create pki enrollmentrequest=sw24cer keypair=8
   ```

4. This command uploads the enrollment request from the switch’s file system to a TFTP server. The command assumes that the TFTP server has the IP address 149.88.88.88. (This step could also be performed using Xmodem.)

   ```
   upload method=tftp destfile=c:sw24cer.csr
   server=149.88.88.88 file=sw24cer.csr
   ```

5. These commands download the CA certificates into the switch's file system from the TFTP server. The commands assume that the IP address of the server is 149.88.88.88 and that the certificate names are "sw24cer.cer" and "ca.cer". (This step could be performed using Xmodem.)

   ```
   load method=tftp destfile=sw24cer.cer server=149.88.88.88
   file=c:sw24cer.cer

   load method=tftp destfile=ca.cer server=149.88.88.88
   file=c:ca.cer
   ```

6. These commands load the certificates into the certificate database:

   ```
   add pki certificate="Switch 24 certificate"
   location=sw24cert.cer

   add pki certificate="CA certificate" location=ca.cer
   ```

7. This command disables the web server:

   ```
   disable http server
   ```

8. This command configures the web server. It activates HTTPS and specifies the key created in step 1:

   ```
   set http server security=enabled sslkeyid=8
   ```

9. This command enables the web server:

   ```
   enable http server
   ```

SHOW HTTP SERVER

Syntax

```
show http server
```

Parameters

None.

Description

This command displays the following information about the web server on the switch:

- Status
- SSL security
- SSL key ID
- Listen port

Example

The following command displays the status of the web server:

```
show http server
```

Chapter 36

Encryption Key Commands

This chapter contains the following commands:

- “CREATE ENCO KEY” on page 614
- “DESTROY ENCO KEY” on page 618
- “SET ENCO KEY” on page 619
- “SHOW ENCO” on page 620

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S63 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. For background information on this feature, refer to Chapter 33, “Encryption Keys” in the *AT-S63 Management Software Menus Interface User’s Guide*.

CREATE ENCO KEY

Syntax 1

```
create enco key=key-id type=rsa length=value
[description="description"]
```

Syntax 2

```
create enco key=key-id type=rsa [description="description"]
[file=filename.key] [format=hex|ssh|ssh2]
```

Parameters

key — Specifies a key ID. The range is 0 to 65,535. The default is 0. When creating a new key this value must be unique from all other key IDs on the switch.

type — Specifies the type of key, which can only be a random RSA key.

length — Specifies the length of the key in bits. The range is 512 to 1536 bits, in increments of 256 bits (for example, 512, 768, 1024, etc). The default is 512 bits. This parameter is only used when creating a new encryption key pair.

description — Specifies a description for the encryption key. The description can be up to 40 alphanumeric characters. Spaces are allowed. The description must be enclosed in quotes. This parameter, which is optional, is used when creating a new key pair and when importing a public key from the AT-S63 file system to the key database. This parameter should not be used when exporting a public key to the file system.

file — Specifies a filename for the key. The filename must include the ".key" extension. This parameter is used when you are importing or exporting a public key from the key database. This parameter is not used when creating a new encryption key pair.

format — Specifies the format when importing or exporting a public encryption key. The options are:

- hex — Specifies a hexadecimal format used to transfer a key between devices other than switches. This is the default.

ssh	Specifies a format for Secure Shell version 1 users.
ssh2	Specifies a format for Secure Shell version 2 users.

Description

This command serves two functions. One is to create encryption keys. The other is to import and export public encryption keys from the AT-S63 file system to the key database.

Caution
Key generation is a CPU-intensive process. Because this process may affect switch behavior, Allied Telesyn recommends creating keys when the switch is not connected to a network or during periods of low network activity.

Syntax 1 Description

Syntax 1 creates encryption key pairs. It creates both the public and private keys of a key pair. A new key pair is automatically stored in the key database and the file system. To view the current keys on a switch, use the "SHOW ENCO" on page 620.

The KEY parameter specifies the identification number for the key. The number must be unique from all other key pairs already on the switch. The range is 0 to 65,535. This number is used only for identification purposes and not in generating the actual encryption key pair.

The TYPE parameter specifies the type of key to be created. The only option is RSA.

The LENGTH parameter specifies the length of the key in bits. The range is 512 to 1,536 bits, in increments of 256 bits (for example, 512, 768, 1024, etc). Before selecting a key length, note the following:

- For SSL and web browser encryption, key length can be any valid value within the range.
- For SSH host and server key pairs, the two key pairs must be created separately and be of different lengths of at least one increment (256 bits) apart. The recommended length for the server key is 768 bits and the recommended length for the host key is 1024 bits.

The DESCRIPTION parameter is optional. You can use it to add a description to the key. This can help you identify the different keys on the switch. The description can be up to forty alphanumeric characters. It must be enclosed in quotes and spaces are allowed.

Syntax 1 Examples

This example creates a key with the ID of 12 and a length of 512 bits:

```
create enco key=12 type=rsa length=512
```

This example creates a key with the ID of 4, a length of 1024 bits, and a description of “Switch12a encryption key”:

```
create enco key=4 type=rsa length=1024
description="Switch12a encryption key"
```

Syntax 2 Description

Syntax 2 is used to import and export public encryption keys. You can import a public key from the AT-S63 file system to the key database or vice versa.

The only circumstance in which you are likely to use this command is if you are using an SSH client that does not download the key automatically when you start an SSH management session. In that situation, you can use this procedure to export the SSH client key from the key database into the AT-S63 file system, from where you can upload it onto the SSH management session for incorporation in your SSH client software.

You should not use this command to export an SSL public key. Typically, an SSL public key only has value when incorporated into a certificate or enrollment request.

The KEY parameter specifies the identification number for the key. The range is 0 to 65,535. To import a public key from the file system to the key database, the key ID must be unused; it cannot already be assigned to another key pair. Importing a public key to the database assumes that you have already stored the public key in the file system.

If you are exporting a public key from the key database to the file system, the KEY parameter should specify the ID of the key that you want to export. Only the public key of a key pair is exported to the file system. You cannot export a private key.

The TYPE parameter specifies the type of key to be imported or exported. The only option is RSA.

The FILE parameter specifies the filename of the encryption key. The filename must include the “.key” extension. If you are exporting a key from the key database to the file system, the filename must be unique from all other files in the file system. If you are importing a key, the filename should specify the name of the file in the file system that contains the key you want to import into the key database.

The DESCRIPTION parameter specifies a user-defined description for the

key. This parameter should be used only when importing a key and not when exporting a key. The description will appear next to the key when you view the key database. Descriptions can help you identify the different keys stored in the switch.

The FORMAT parameter specifies the format of the key, which can be either Secure Shell format (SSH version 1 or 2) or hexadecimal format (HEX). The FORMAT parameter must be specified when importing or exporting keys. The default is HEX.

Syntax 2 Examples

This is an example of exporting a public key from the key database to the file system. The example assumes that the ID of the key pair with the public key to be exported is 12 and that you want to store the key as a file called "public12.key" in the file system. It specifies the format as SSH version 1 and the type as RSA:

```
create enco key=12 type=rsa file=public12.key format=ssh
```

This is an example of importing a public key from the file system to the key database. It assumes that the name of the file containing the public key is swpub24.key and that the key is to be given the ID number 6 in the key database. It gives the key the description "Switch 24 public key." The format is SSH version 2 and the type is RSA:

```
create enco key=6 type=rsa description="Switch 24 public
key" file=swpub24.key format=ssh2
```

DESTROY ENCO KEY

Syntax

```
destroy enco key=key-id
```

Parameter

key	Specifies the ID number of the key pair to be deleted from the key database.

Description

This command deletes an encryption key pair from the key database. This command also deletes a key's corresponding ".UKF" file from the file system. After a key pair is deleted, any SSL certificate created using the public key of the key pair will be invalid and cannot be used to manage the switch. To view the keys, see "SHOW ENCO" on page 620.

You cannot delete a key pair if it is being used by SSL or SSH. You must first either disable the SSL or SSH server software on the switch or reconfigure the software by specifying another key.

Example

The following command destroys the encryption key pair with the key ID 4:

```
destroy enco key=4
```

SET ENCO KEY

Syntax

```
set enco key=key-id description="description"
```

Parameters

key	Specifies the ID number of the key pair whose description you want to change.
description	Specifies the new description of the key. The description can contain up to 25 alphanumeric characters. Spaces are allowed. The description must be enclosed in double quotes.

Description

This command changes the description of a key pair. Descriptions can make it easier to identify the different keys on a switch.

The KEY parameter specifies the identification number of the key. The encryption key must already exist. To view the keys on a switch, see "SHOW ENCO" on page 620.

The DESCRIPTION parameter specifies the new description for the key.

Example

The following command changes the description for the key with the ID 6 to "Switch 22 key":

```
set enco key=1 description="Switch 22 key"
```

SHOW ENCO

Syntax

```
show enco key=[key-id]
```

Parameters

key	Specifies the ID of a specific key whose information you want to display. Otherwise, all keys are displayed.

Description

This command displays information about encryption key pairs stored in the key database. This command displays the following information about each key:

- ID
- Algorithm
- Length Digest
- Description

Example

The following command displays the information on encryption key 1:

```
show enco key=1
```

Chapter 37

Public Key Infrastructure (PKI) Certificate Commands

This chapter contains the following commands:

- "ADD PKI CERTIFICATE" on page 622
- "CREATE PKI CERTIFICATE" on page 624
- "CREATE PKI ENROLLMENTREQUEST" on page 627
- "DELETE PKI CERTIFICATE" on page 629
- "PURGE PKI" on page 630
- "SET PKI CERTIFICATE" on page 631
- "SET PKI CERTSTORELIMIT" on page 633
- "SET SYSTEM DISTINGUISHEDNAME" on page 634
- "SHOW PKI" on page 635
- "SHOW PKI CERTIFICATE" on page 636

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S63 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. For background information on this feature, refer to Chapter 34, "PKI Certificates and SSL" in the *AT-S63 Management Software Menus Interface User's Guide*.

ADD PKI CERTIFICATE

Syntax

```
add pki certificate="name" location="filename.cer"
[trusted=yes|no|on|off|true|false] [type=ca|ee|self]
```

Parameters

certificate — Specifies a name for the certificate. This is the name for the certificate as it will appear in the certificate database list. The name can up to 40 alphanumeric characters. Spaces are allowed. If the name contains spaces, it must be enclosed in double quotes. Each certificate must be given a unique name.

location — Specifies the filename of the certificate, with the ".cer" file extension, as it is stored in the switch's file system.

trusted — Specifies whether or not the certificate is from a trusted CA. The options are:

- yes, on, true — Specifies that the certificate is from a trusted CA. This is the default.
- no, off, false — Specifies that the certificate is not from a trusted CA.

type — Specifies the type of certificate being added. The options are:

- ca — Tags the certificate as a CA certificate.
- ee — Tags the certificate as belonging to another end entity (EE). This is the default.
- self — Tags the certificate as its own.

Description

This command adds a certificate to the certificate database from the AT-S63 file system. To view the certificate files in the file system, refer to "SHOW FILE" on page 223. To view the certificates already in the database, refer to "SHOW PKI CERTIFICATE" on page 636.

The CERTIFICATE parameter assigns the certificate a name. The name can be from 1 to 40 alphanumeric characters. Each certificate in the database should be given a unique name.

The LOCATION parameter specifies the filename of the certificate as stored in the switch's file system. When specifying the filename, be sure to include the file extension ".cer".

The TRUSTED parameter specifies whether the certificate is from a trusted CA. The default is TRUE. Only self-signed root CA certificates are typically set to be automatically trusted, and only after the user has checked the certificate's fingerprint and other details using "SHOW PKI CERTIFICATE" on page 636.

The TYPE parameter specifies what type of certificate is being added. Self signed certificates should be assigned a type of SELF. If CA is specified, the switch tags this certificate as a CA certificate. If ENDENTITY or EE is specified, the switch tags the certificate to indicate that it belongs to an end entity. The default is ENDENTITY.

Note
The TRUSTED and TYPE parameters have no affect on the operation of a certificate. You can select any permitted value for either parameter, or you can omit the parameters. The parameters are included only as placeholders for information in the certificate database.

Example

The following command loads the certificate "sw12.cer" from the file system into the certificate database. The certificate is assigned the name "Switch 12 certificate":

```
add pki certificate="Switch 12 certificate"
location="sw12.cer" type=self
```

CREATE PKI CERTIFICATE

Syntax

```
create pki certificate=name keypair=key-id
serialnumber=value [format=der|pem]
subject="distinguished-name"
```

Parameters

certificate	Specifies a name for the self-signed certificate. The name can be from one to eight alphanumeric characters. Spaces are allowed; if included, the name must be enclosed in double quotes. The management software automatically adds the ".cer" extension.
keypair	Specifies the ID of the key pair that you want to use to create the certificate.
serialnumber	Specifies the serial number for the certificate. The range is 0 to 2147483647. The default is 0.
format	Specifies the type of encoding the certificate will use. The options are:
	der — Specifies binary format which cannot be displayed. This is the default.
	pem — Specifies an ASCII-encoded format that allows the certificate to be displayed once it is generated.
subject	Specifies the distinguished name for the certificate. The name must be enclosed in quotes.

Description

This command creates a self-signed certificate. You can use the certificate to add encryption to your web browser management sessions of the switch. A new self-signed certificate is automatically stored in the switch's file system.

Before you can create a self-signed certificate, you must create an encryption key pair. The certificate will contain the public key of the key pair. To create a key pair, refer to "CREATE PKI CERTIFICATE" on page 624.

After you have created a new self-signed certificate, you need to load it into the certificate database. The switch cannot use the certificate for

encrypted web browser management systems until it is loaded into the database. For instructions, refer to "ADD PKI CERTIFICATE" on page 622.

Note
For a review of the steps to configuring the web server for a self-signed certificate, refer to "SET HTTP SERVER" on page 607.

The CERTIFICATE parameter assigns a file name to the certificate. This is the name under which the certificate will be stored as in the switch's file system. The name can be from one to eight alphanumeric characters. If the name includes a space, it must be enclosed in double quotes. The software automatically adds the extension ".cer" to the name.

The KEYPAIR parameter specifies the ID of the encryption key that you want to use to create the certificate. The public key of the pair will be incorporated into the certificate. The key pair that you select must already exist on the switch. To create a key pair, refer to "CREATE ENCO KEY" on page 614. To view the IDs of the keys already on the switch, refer to "SHOW ENCO" on page 620.

The SERIALNUMBER parameter specifies the number to be inserted into the serial number field of the certificate. A serial number is typically used to distinguish a certificate from all others issued by the same issuer, in this case the switch. Self-signed certificates are usually assigned a serial number of 0.

The FORMAT parameter specifies the type of encoding the certificate will use. PEM is ASCII-encoded and allows the certificate to be displayed once it has been generated. DER encoding is binary and so cannot be displayed. The default is DER.

The SUBJECT parameter specifies the distinguished name for the certificate. The name is inserted in the subject field of the certificate. Allied Telesyn recommends using the IP address of the master switch as the distinguished name (for example, "cn=149.11.11.11"). If your network has a Domain Name System and you mapped a name to the IP address of a switch, you can specify the switch's name instead of the IP address as the distinguished name. For a explanation of distinguished names, refer to Chapter 34, "PKI Certificates and SSL" in the *AT-S63 Management Software Menus Interface User's Guide*.

Examples

The following command creates a self-signed certificate. It assigns the certificate the filename “sw12.cer”. (The management software automatically adds the “.cer” extension.) The command uses the key pair with the ID 12 to create the certificate. The format is ASCII and the distinguished name is the IP address of a master switch:

```
create pki certificate=sw12 keypair=12 serialnumber=0
format=pem subject="cn=149.11.11.11"
```

The following command creates a self-signed certificate with a filename of “S45 cert”. The key pair used to create it has the ID 5. No format is specified, so the default binary format is used. The distinguished name is the IP address of another master switch:

```
create pki certificate="S45 cert" keypair=5 serialnumber=0
subject="cn=149.22.22.22"
```

CREATE PKI ENROLLMENTREQUEST

Syntax

```
create pki enrollmentrequest="name" keypair=key-id
[format=der|pem] [type=pkcs10]
```

Parameters

enrollmentrequest	Specifies a filename for the enrollment request. The filename can be from 1 to 8 alphanumeric characters. If the name contains spaces, it must be enclosed in double quotes. The management software automatically adds the ".csr" extension.
keypair	Specifies the key pair that you want to use to create the enrollment request.
format	Specifies the type of encoding the certificate request will use. The options are: der — Specifies binary format which cannot be displayed. This is the default. pem — Specifies an ASCII-encoded format that allows the certificate to be displayed once it is generated.
type	Formats the request according to PKCS #10.

Description

This command creates a certificate enrollment request. You create an enrollment request when you want a public or private CA to issue a certificate.

Before you can create an enrollment request, you must create the key pair that you want the CA to use when creating the certificate. The enrollment request will contain the public key of the key pair. To create a key pair, refer to "CREATE PKI CERTIFICATE" on page 624.

You must also set the system's distinguished name before using this command. For a explanation of distinguished names, refer to Chapter 34, "PKI Certificates and SSL" in the *AT-S63 Management Software Menus Interface User's Guide*. To set the distinguished name, refer to "SET SYSTEM DISTINGUISHEDNAME" on page 634.

Note
For a review of the steps to configuring the web server for a CA certificate, refer to “SET HTTP SERVER” on page 607.

The ENROLLMENTREQUEST parameter specifies a filename for the request. The filename can contain from 1 to 8 alphanumeric characters. If spaces are used, the name must be enclosed in quotes. The management software automatically adds the “.csr” extension. This is the filename under which the request will be stored in the file system.

The KEYPAIR parameter specifies the key that you want to use to create the enrollment request. The public key of the pair is incorporated into the request.

The FORMAT parameter specifies the type of encoding format for the request. DER specifies that the enrollment request should be written straight to the binary file. PEM specifies that the enrollment request should be encoded using the “Privacy Enhanced Mail” format. The default is DER. This parameter is only valid for manual enrollment.

The TYPE parameter specifies the type of request. The only option is PKCS10.

You do not need to use the SAVE CONFIGURATION command after you create an enrollment request. The file is permanently saved in the file system until you manually delete it.

Examples

The following command creates an enrollment request. It names the enrollment request file “Switch12” and uses the key pair with the ID 4 to generate the request:

```
create pki enrollmentrequest=Switch12 keypair=4
```

DELETE PKI CERTIFICATE

Syntax

```
delete pki certificate="name"
```

Parameter

certificate	Specifies the name of the certificate you want to delete from the certificate database. The name is case sensitive. If the name contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Description

This command deletes a certificate from the switch's certificate database. To view the certificates in the database, refer to "SHOW PKI CERTIFICATE" on page 636.

Deleting a certificate from the database does not delete it from the file system. To delete a file from the file system, refer to "DELETE FILE" on page 213.

You cannot delete a certificate from the database if you specified its corresponding encryption key as the active key in the web server configuration. The switch considers the certificate to be in use and will not allow you to delete it. You must first configure the web server with another encryption key pair for a different certificate.

Example

The following command deletes the certificate "Switch 12 certificate" from the certificate database:

```
delete pki certificate="Switch 12 certificate"
```

PURGE PKI

Syntax

```
purge pki
```

Parameters

None.

Description

This command deletes all certificates from the certificate database and resets the certificate database storage limit to the default. This command does not delete the certificates from the file system. To delete files from the file system, refer to “DELETE FILE” on page 213.

Example

The following command deletes the certificates from the database and resets the storage limit to the default:

```
purge pki
```

SET PKI CERTIFICATE

Syntax

```
set pki certificate="name"
[trusted=yes|no|on|off|true|false] [type=ca|ee|self]
```

Parameters

certificate — Specifies the certificate name whose trust or type you want to change. The name is case sensitive. If the name contains spaces, it must be enclosed in quotes.

trusted — Specifies whether or not the certificate is from a trusted CA. The options are:

- yes, on, true — Specifies that the certificate is from a trusted CA. This is the default. The options are equivalent.
- no, off, false — Specifies that the certificate is not from a trusted CA. The options are equivalent.

type — Specifies a type for the certificate. The options are:

- ca — Tags the certificate as a CA certificate.
- ee — Tags the certificate as belonging to another end entity (EE). This is the default.
- self — Tags the certificate as its own.

Description

This command changes the level of trust and type for a certificate in the switch's certificate database. To list the certificates in the database, refer to "SHOW PKI CERTIFICATE" on page 636.

The TRUSTED parameter specifies whether the certificate is from a trusted CA. The default is TRUE. Only self-signed root CA certificates are typically set to be automatically trusted, and only after the user has checked the certificate's fingerprint and other details using "SHOW PKI CERTIFICATE" on page 636.

The TYPE parameter specifies the certificate type. If CA is specified, the switch tags this certificate as a CA certificate. If ENDENTITY or EE is specified, the switch tags the certificate to indicate that it belongs to an end entity. If SELF is specified, the switch tags the certificate as its own. The default is ENDENTITY.

Note
The TRUSTED and TYPE parameters have no affect on the operation of a certificate. You can select any permitted value for either parameter. The parameters are included only as placeholders for information in the certificate database.

Example

The following command sets the certificate named “Switch 12 certificate” to be trusted.

```
set pki certificate="Switch 12 certificate" trusted=true
```

SET PKI CERTSTORELIMIT

Syntax

```
set pki certstorelimit=value
```

Parameter

certstorelimit — Specifies the maximum number of certificates that can be stored in the certificate database. The range is 12 and 256; the default is 256.

Description

This command sets the maximum number of certificates that can be stored in the switch's certificate database.

Example

The following command sets the certificate storage limit to 100:

```
set pki certstorelimit=100
```

SET SYSTEM DISTINGUISHEDNAME

Syntax

```
set system distinguishedname="name"
```

Parameter

distinguishedname	Specifies the distinguished name for the switch. The name must be enclosed in quotes.

Description

This command sets the distinguished name for the switch. The distinguished name is used to create a self signed certificate or enrollment request. For a explanation of distinguished names, refer to Chapter 34, “PKI Certificates and SSL” in the *AT-S63 Management Software Menus Interface User’s Guide*.

Allied Telesyn recommends using the switch’s IP address or, for networks with a Domain Name System, its domain name as the distinguished name. For slave switches, which do not have an IP address, you can use the IP address or domain name of the master switch of the enhanced stack as the slave switch’s distinguished name.

To set the distinguished name when creating a self signed certificate, you can use this command or you can set it directly in “CREATE PKI CERTIFICATE” on page 624, which is the command for creating a self signed certificate. It has a parameter for setting the distinguished name.

If you are creating an enrollment request, you must set the distinguished name with this command first before creating the request. The command for creating an enrollment request is “CREATE PKI ENROLLMENTREQUEST” on page 627.

Example

The following command sets the switch’s distinguished name to the IP address 169.22.22.22:

```
set system distinguishedname="cn=169.22.22.22"
```

SHOW PKI

Syntax

```
show pki
```

Parameters

None.

Description

This command displays the current setting for the maximum number of certificates the switch will allow you to store in the certificate database. To change this value, refer to "SET PKI CERTSTORELIMIT" on page 633.

Example

The following command displays the current PKI settings:

```
show pki
```

SHOW PKI CERTIFICATE

Syntax

```
show pki certificate[="name"]
```

Parameter

certificate	Specifies the name of the certificate whose information you want to view. If the name contains spaces, it must be enclosed in double quotes. This parameter is case sensitive. Wildcards are not allowed.

Description

This command lists all of the certificates in the certificates database. This command can also display information about a specific certificate in the database.

Example

The following command lists all of the certificates in the database:

```
show pki certificate
```

The following command displays information specific to the certificate “Switch 12 certificate”:

```
show pki certificate="Switch 12 certificate"
```

Chapter 38

Secure Sockets Layer (SSL) Commands

This chapter contains the following command:

- “SET SSL” on page 638
- “SHOW SSL” on page 639

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S63 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. For background information on this feature, refer to Chapter 34, “PKI Certificates and SSL” in the *AT-S63 Management Software Menus Interface User’s Guide*.

SET SSL

Syntax

```
set ssl [cachetimeout=value] [maxsessions=value]
```

Parameters

cachetimeout	Specifies the maximum time in seconds that a session will be retained in the cache The range is 1 to 600 seconds. The default is 300 seconds.
maxsessions	Specifies the maximum number of sessions that will be allowed in the session resumption cache. The range is 0 to 100 sessions. The default is 50 sessions.

Description

This command configures the SSL parameters.

The CACHETIMEOUT parameter determines the maximum time that a session will be retained in the cache. The cache stores information about closed connections so they can be resumed quickly. The default is 300 seconds.

The MAXSESSIONS parameter specifies the maximum number of sessions that will be allowed in the session resumption cache. The number of ENCO channels supported by the switch limits this number. The default is 50 sessions.

Example

The following command sets the session resumption cache to 180 seconds:

```
set ssl cachetimeout=180
```

SHOW SSL

Syntax

```
show ssl
```

Parameters

None.

Description

This command displays the current settings for the following SSL values:

- Version
- Available ciphers
- Maximum number of sessions
- Cache timeout

Example

The following command displays the current SSL settings:

```
show ssl
```

Chapter 39

Secure Shell (SSH) Commands

This chapter contains the following commands:

- “DISABLE SSH SERVER” on page 642
- “ENABLE SSH SERVER” on page 643
- “SET SSH SERVER” on page 646
- “SHOW SSH” on page 648

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S63 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. For background information on this feature, refer to Chapter 35, “Secure Shell (SSH)” in the *AT-S63 Management Software Menus Interface User’s Guide*.

DISABLE SSH SERVER

Syntax

```
disable ssh server
```

Parameters

None.

Description

This command disables the Secure Shell server. When the Secure Shell server is disabled, connections from Secure Shell clients are not accepted.

By default, the Secure Shell server is disabled.

Example

The following command disables the Secure Shell server:

```
disable ssh server
```

ENABLE SSH SERVER

Syntax

```
enable ssh server hostkey=key-id serverkey=key-id
[expirytime=hours] [logintimeout=seconds]
```

Parameters

hostkey	Specifies the ID number of the encryption key pair to function as the host key.
serverkey	Specifies the ID number of the encryption key pair to function as the server key.
expirytime	Specifies the length of time, in hours, after which the server key pair is regenerated. The range is 0 to 5 hours. Entering 0 never regenerates the key. The default is 0.
logintimeout	Specifies the length of time the server waits before disconnecting an un-authenticated client. The range is 60 to 600 and the default is 180.

Description

This command enables the Secure Shell server and sets the server's parameters. When the Secure Shell server is enabled, connections from Secure Shell clients are accepted. The default setting for the server is disabled.

The HOSTKEY parameter specifies the key ID of the host key pair. The specified key pair must already exist. To create a key pair, refer to "CREATE ENCO KEY" on page 614 (syntax 1).

The SERVERKEY parameter specifies the key of the server key pair. The specified key pair must already exist.

The EXPIRYTIME parameter specifies the time, in hours, after which the Secure Shell server key will expire and will be regenerated. If 0 is specified the key does not expire. The range is 0 to 5 and the default is 0.

The LOGINTIMEOUT parameter specifies the length of time the server waits before disconnecting an unauthenticated client. The range is 60 to 600 and the default is 180.

Note
Before you enable SSH, disable the Telnet management session. Otherwise, the security provided by SSH is not active. See “DISABLE TELNET” on page 45.

Example

The following command activates the Secure Shell server and specifies encryption key pair 0 as the host key and key pair 1 as the server key:

```
enable ssh server hostkey=0 serverkey=1
```

General Configuration Steps for SSH Operation

Configuring the SSH server involves several commands. The information in this section lists the functions and commands you need to perform to configure the SSH feature.

1. Create two encryption key pairs. One pair will function as the SSH host key and another as the SSH server key. The keys must be of different lengths of at least one increment (256 bits) apart. The recommended size for the server key is 768 bits. The recommended size for the server key is 1024 bits. To create a key pair, see to “CREATE ENCO KEY” on page 614.

2. Disable Telnet access to the switch with the DISABLE TELNET command. See “DISABLE TELNET” on page 45.

   Although the AT-S63 management software allows the SSH and Telnet servers to be active on the switch simultaneously, allowing Telnet to remain active negates the security of the SSH feature.

3. Configure and activate SSH on the switch using “ENABLE SSH SERVER” on page 643.

4. Install SSH client software on your PC.

   Follow the directions provided with the client software. You can download SSH client software from the Internet. Two popular SSH clients are PuTTY and CYGWIN.

5. Log on to the SSH server from the SSH client.

   Acceptable users are those with a Manager or Operator login as well as users configured with the RADIUS and TACACS+ protocols.

Example

The following is an example of the command sequence to configuring the SSH software on the server:

1. The first step is to create the two encryption key pairs. Each key must be created separately and the key lengths must be at least one increment (256 bits) apart. The following two commands create the host and server keys using the recommended key lengths:

   ```
   create enco key=1 type=rsa length=1024 description="host key"

   create enco key=2 type=rsa length=768 description="server key"
   ```

2. The following command disables Telnet:

   ```
   disable telnet
   ```

3. The last command activates the SSH software and sets the host key as encryption key pair 1 and the server key as key pair 2:

   ```
   enable ssh server hostkey=1 serverkey=2
   ```

SET SSH SERVER

Syntax

```
set ssh server hostkey=key-id serverkey=key-id
[expirytime=hours] [logintimeout=seconds]
```

Parameters

hostkey	Specifies the ID number of the encryption key pair to function as the host key.
serverkey	Specifies the ID number of the encryption key pair to function as the server key.
expirytime	Specifies the length of time, in hours, after which the server key pair is regenerated. The range is 0 to 5 hours. Entering 0 never regenerates the key. The default is 0.
logintimeout	Specifies the length of time the server waits before disconnecting an un-authenticated client. The range is 60 to 600 and the default is 180.

Description

This command modifies the configuration of the Secure Shell server parameters.

The HOSTKEY parameter specifies the key ID of the host key pair. The specified key pair must already exist. To create a key pair, refer to “CREATE ENCO KEY” on page 614 (syntax 1).

The SERVERKEY parameter specifies the key of the server key pair. The specified key pair must already exist.

The EXPIRYTIME parameter specifies the time, in hours, after which the Secure Shell server key will expire and will be regenerated. If 0 is specified the key does not expire. The range is 0 to 5 and the default is 0.

The LOGINTIMEOUT parameter specifies the length of time the server waits before disconnecting an un-authenticated client. The range is 60 to 600 seconds. The default is 180 seconds.

Example

The following command sets the Secure Shell server key expiry time to 1 hour:

```
set ssh server expirytime=1
```

SHOW SSH

Syntax

```
show ssh
```

Parameters

None.

Description

This command displays the current values for the following SSH parameters:

- Versions supported
- Server Status
- Server Port
- Host Key ID
- Host Key Bits (size of host key in bits)
- Server Key ID
- Server Key Bits (size of server key in bits)
- Server Key Expiry (hours)
- Login Timeout (seconds)
- Authentication Available
- Ciphers Available
- MACs Available
- Data Compression

Example

The following command displays the configuration of the Secure Shell server:

```
show ssh
```

Chapter 40
TACACS+ and RADIUS Commands

This chapter contains the following commands:

- “ADD RADIUSSERVER” on page 650
- “ADD TACACSSERVER” on page 652
- “DELETE RADIUSSERVER” on page 653
- “DELETE TACACSSERVER” on page 654
- “DISABLE AUTHENTICATION” on page 655
- “ENABLE AUTHENTICATION” on page 656
- “PURGE AUTHENTICATION” on page 657
- “SET AUTHENTICATION” on page 658
- “SHOW AUTHENTICATION” on page 660

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on these features, refer to Chapter 36, “TACACS+ and RADIUS Protocols” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD RADIUSSERVER

Syntax

```
add radiusserver server|ipaddress=ipaddress order=value
[secret=string] [port=value] [accport=value]
```

Parameters

server ***or*** ipaddress	Specifies an IP address of a RADIUS server. The parameters are equivalent.
order	Specifies the order that the RADIUS servers are queried by the switch. This value can be from 1 to 3. The servers are queried starting with 1.
secret	Specifies the encryption key used for this server. The maximum length is 39 characters.
port	Specifies the UDP (User Datagram Protocol) port of the RADIUS server. The default is port 1812.
accport	Specifies the UDP port for RADIUS accounting. The default is port 1813.

Description

This command specifies the IP addresses of RADIUS servers and the order they are to be queried by the switch. There can be up to three servers, but you must specify each one individually with this command. You may specify an encryption key, a RADIUS UDP port, and a RADIUS accounting UDP port.

Examples

The following command adds a RADIUS server with the 149.245.22.22 IP address and specifies it as the first server in the list:

```
add radiusserver ipaddress=149.245.22.22 order=1
```

The following command adds the RADIUS server with the IP address 149.245.22.22. In addition, it specifies the server as the third RADIUS server to be queried by the switch and has a UDP port of 3:

```
add radiusserver ipaddress=149.245.22.22 order=3 port=3
```

The following command adds a RADIUS server with an IP address of 149.245.22.22. It specifies the order is 2, the encryption key is tiger74, and the UDP port is 1811:

```
add radiusserver ipaddress=149.245.22.22 order=2
secret=tiger74 port=1811
```

ADD TACACSSERVER

Syntax

```
add tacacsserver server|ipaddress=ipaddress order=value
[secret=string]
```

Parameters

server ***or*** ipaddress	Specifies an IP address of a TACACS+ server. The parameters are equivalent.
order	Specifies the order that your TACACS+ servers are queried by the switch. You can assign order to up to 3 servers with 1 being the first server queried.
secret	Specifies the optional encryption key used on this server. The maximum length is 39 characters.

Description

This command adds the IP addresses of TACACS+ servers to your switch along with the order the TACACS+ servers are to be queried and an optional encryption key.

Examples

The following command adds a TACACS+ server with an IP address 149.245.22.20 and an order value of 1:

```
add tacacsserver ipaddress=149.245.22.20 order=1
```

The following command adds a TACACS+ server with an IP address of 149.245.22.24, an order of 2, and an encryption code of lioness54:

```
add tacacsserver ipaddress=149.245.22.24 order=2
secret=lioness54
```

The following command adds a TACACS+ server with an IP address 149.245.22.26 and specifies that this TACACS+ server is the third TACACS+ server to be queried by the switch:

```
add tacacsserver ipaddress=149.245.22.26 order=3
```

DELETE RADIUSSERVER

Syntax

```
delete radiusserver server|ipaddress=ipaddress
```

Parameter

server ***or*** ipaddress	Specifies the IP address of a RADIUS server to be deleted from the management software. The parameters are equivalent.

Description

This command deletes the IP address of a RADIUS from your switch.

Example

The following command deletes the RADIUS server with the IP address 149.245.22.22:

```
delete radiusserver ipaddress=149.245.22.22
```

DELETE TACACSSERVER

Syntax

```
delete tacacsserver server|ipaddress=ipaddress
```

Parameter

server ***or*** ipaddress	Specifies the IP address of a TACACS+ server to be deleted from the management software. The parameters are equivalent.

Description

This command deletes the IP address of a TACACS+ server from your switch.

Example

The following command deletes the TACACS+ server with the IP address 149.245.22.20:

```
delete tacacsserver ipaddress=149.245.22.20
```

DISABLE AUTHENTICATION

Syntax

```
disable authentication
```

Parameters

None.

Description

This command disables TACACS+ and RADIUS manager account authentication on your switch. When you disable authentication you retain your current authentication parameter settings.

Note
This command applies only to TACACS+ and RADIUS manager accounts. Disabling authentication means that you must use the default manager accounts of manager and operator to manage the switch. This command does not affect 802.1x port-based access control.

Example

The following command disables TACACS+ and RADIUS manager account authentication on your switch:

```
disable authentication
```

ENABLE AUTHENTICATION

Syntax

```
enable authentication
```

Parameters

None.

Description

This command enables TACACS+ or RADIUS manager account authentication on your switch. You must use the manager accounts you defined on the TACACS+ or RADIUS server to manage the switch when you enable manager authentication. To select an authenticator protocol, refer to “SET AUTHENTICATION” on page 658.

> **Note**
> If you are using the RADIUS authentication protocol for 802.1x Port-based Network Access Control but not for manager account authentication, you do not need to use this command. You can leave the RADIUS manager account feature disabled. The switch still has access to the RADIUS configuration information for 802.1x port-based access control.

Example

The following command enables manager account authentication on your switch:

```
enable authentication
```

PURGE AUTHENTICATION

Syntax

```
purge authentication
```

Parameters

None.

Description

This command disables authentication, returns the authentication method to TACACS+, deletes any global secret, and returns the timeout value to its default setting of 10 seconds. This command does not delete the IP address or secret of any RADIUS or TACACS+ authentication servers you may have specified.

Example

The following command returns the authentication settings to their default values:

```
purge authentication
```

SET AUTHENTICATION

Syntax

```
set authentication method=tacacs|radius [secret=string]
[timeout=value]
```

Parameters

method	Specifies which authenticator protocol, TACACS+ or RADIUS, is to be the active protocol on the switch.
secret	Specifies the global encryption key of the TACACS+ or RADIUS servers. If the servers use different encryption keys, you can leave this parameter blank and set individual encryption keys with "ADD TACACSSERVER" on page 652 or "ADD RADIUSSERVER" on page 650. To remove a previously assigned global key without specifying a new value, enter the string as "none". The maximum length is 39 characters.
timeout	Specifies the maximum amount of time the switch waits for a response from an authentication server before the switch assumes the server will not respond. If the timeout expires and the server has not responded, the switch queries the next server in the list. After the switch has exhausted the list of servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 300 seconds.

Description

This command selects the authentication protocol. One authentication protocol can be active on the switch at a time. You may specify a global encryption code and the maximum number of seconds the switch waits for a response from an authenticator server.

Examples

The following command selects TACACS+ as the authentication protocol on the switch:

```
set authentication method=tacacs
```

The following command selects TACACS+ as the authentication protocol and specifies a global encryption key of tiger54:

```
set authentication method=tacacs secret=tiger54
```

The following command selects RADIUS as the authentication protocol with a global encryption key of leopard09 and a timeout of 15 seconds:

```
set authentication method=radius secret=leopard09 timeout=15
```

The following command removes the current global secret from the RADIUS client without assigning a new value:

```
set authentication method=radius secret=none
```

SHOW AUTHENTICATION

Syntax

```
show authentication[=tacacs|radius]
```

Parameters

None.

Description

This command displays the following information about the authenticated protocols on the switch:

- Status - The status of your authenticated protocol: enabled or disabled.
- Authentication Method - The authentication protocol activated on your switch. Either TACACS+ or RADIUS protocol may be active. The TACACS+ protocol is the default.
- The IP addresses of up to three authentication servers.
- The server encryption keys, if defined.
- TAC global secret - The global encryption code that applies to all authentication servers.
- Timeout - The length of the time, in seconds, before the switch assumes the server will not respond.

Entering the command without specifying either TACACS or RADIUS displays the current status of the authentication feature and the specifics of the currently selected authentication protocol. Specifying TACACS or RADIUS in the command displays the specifics for that authentication protocol.

Example

The following command displays authentication protocol information on your switch:

```
show authentication
```

The following command displays the information for the RADIUS protocol:

```
show authentication=radius
```

Chapter 41

Management ACL Commands

This chapter contains the following commands:

- “ADD MGMTACL” on page 662
- “CREATE MGMTACL” on page 663
- “DESTROY MGMTACL” on page 665
- “DISABLE MGMTACL” on page 666
- “ENABLE MGMTACL” on page 667
- “PURGE MGMTACL” on page 668
- “SET MGMTACL” on page 669
- “SHOW MGMTACL” on page 670

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on this feature, refer to Chapter 37, “Management Access Control List” in the *AT-S63 Management Software Menus Interface User’s Guide*.

ADD MGMTACL

Syntax

```
add mgmtacl id=value application=telnet|web|ping|all
```

Parameters

id — Specifies the identification number of the access control entry to be modified. The range is 1 to 256. To view the ID numbers of the existing ACEs, refer to “SHOW MGMTACL” on page 670.

application — Specifies the permitted applications of the ACE. The options are:

- telnet — Permits Telnet management.
- web — Permits web browser management.
- ping — Permits the management workstation to ping the switch.
- all — Permits all of the above.

You can specify more than one option by separating them with a comma (for example, “Web,Ping”). The new application is added to the existing application of the ACE.

Description

This command modifies the permitted application of an ACE. The new application is added to any application already assigned to the ACE. If you want to assign a new application while overriding the existing one, refer to “SET MGMTACL” on page 669.

Examples

The following command adds web browser as a permitted application to ACE ID 12:

```
add mgmtacl id=12 application=web
```

The following command adds pinging as a permitted application to ACE ID 27:

```
add mgmtacl id=27 application=ping
```

CREATE MGMTACL

Syntax

```
create mgmtacl id=value ipddress=ipaddress mask=string
application=telnet|web|ping|all
```

Parameters

id — Specifies an identification number for the new access control entry. The range is 1 to 256. Every ACE must have a unique identification number.

ipaddress — Specifies the IP address of a subnet or a specific management station.

mask — Specifies the mask used by the switch to filter the IP address. A binary "1" indicates the switch should filter on the corresponding bit of the address, while a "0" indicates that it should not. If, with the IPADDRESS parameter, you specify the IP address of a specific management station, the appropriate mask is 255.255.255.255. If you are filtering on a subnet, then the mask would depend on the address. For example, for a Class C subnet address of 149.11.11.32, the mask would be 255.255.255.224.

application — Specifies the permitted type of remote management. The options are:

- telnet — Permits Telnet management.
- web — Permits web browser management.
- ping — Permits the management workstation to ping the switch.
- all — Permits all of the above.

You can specify more than one option by separating them with a comma (for example, "Web,Ping").

Description

This command creates a new access control entry for the Management ACL. The Management ACL controls who can manage the switch remotely using a web browser or the Telnet application protocol. There can be up to 256 ACEs in a Management ACL.

An ACE is an implicit “permit” statement. A workstation that meets the criteria of the ACE is allowed to remotely manage the switch.

The IPADDRESS parameter specifies the IP address of a specific management station or a subnet.

The MASK parameter indicates the parts of the IP address the switch should filter on. A binary “1” indicates the switch should filter on the corresponding bit of the address, while a “0” indicates that it should not. If you are filtering on a specific IP address, use the mask 255.255.255.255. For a subnet, you need to enter the appropriate mask. For example, to allow all management stations in the subnet 149.11.11.0 to manage the switch, you would enter the mask 255.255.255.0.

The APPLICATION parameter allows you control whether the remote management station can manage the switch using Telnet, a web browser, or both. You can also use it to control whether the workstation can ping the device. For example, you might create an ACE that states that a particular remote management station can only use a web browser to manage the switch.

Note
You must specify all the parameters when creating a new entry.

Examples

The following command creates an ACE that allows the management station with the IP address 169.254.134.247 to manage the switch from either a Telnet or web browser management session and to ping the device:

```
create mgmtacl id=1 ipaddress=169.254.134.247
mask=255.255.255.255 application=all
```

The following command creates an ACE that allows the management station with the IP address 169.254.134.12 to manage the switch with a web browser and to ping the device. However, the workstation cannot manage the switch with the Telnet application protocol:

```
create mgmtacl id=12 ipaddress=169.254.134.12
mask=255.255.255.255 application=web,ping
```

The following command creates an ACE that allows all management stations in the Class A subnet 169.24.144.128 to manage the switch using the Telnet protocol application:

```
create mgmtacl id=17 ipaddress=169.24.144.128
mask=255.255.255.224 application=telnet
```

DESTROY MGMTACL

Syntax

```
destroy mgmtacl id=value
```

Parameters

id — Specifies the identification number of the ACE to be deleted.

Description

This command deletes an ACE from the Management ACL. You specify the ACE by its identification number, which is displayed with "SHOW MGMTACL" on page 670.

Note
If you are remotely managing the switch from a Telnet management session and the Management ACL is active, your management session will end and you will be unable to reestablish it if you delete the ACE that specifies your management workstation.

Example

The following command deletes the ACE with the identification number 18 from the Management ACL:

```
destroy mgmtacl id=18
```

DISABLE MGMTACL

Syntax

```
disable mgmtacl
```

Parameters

None

Description

This command disables the Management ACL.

Example

The following command disables the Management ACL:

```
disable mgmtacl
```

ENABLE MGMTACL

Syntax

```
enable mgmtacl
```

Parameters

None.

Description

This command activates the Management ACL.

> **Note**
> Activating the Management ACL without entering any access control entries (ACEs) prohibits you from remotely managing the switch from a Telnet or web browser management session, or pinging the device.

Example

The following command activates the Management ACL:

```
enable mgmtacl
```

PURGE MGMTACL

Syntax

```
purge mgmtacl
```

Parameters

None.

Description

This command deletes all access control entries from the Management ACL.

> **Note**
> If you are remotely managing the switch from a Telnet management session and the Management ACL is active, your management session will end and you will be unable to reestablish it if you delete all ACEs.

Example

The following command deletes all ACEs from the Management ACL:

```
purge mgmtacl
```

SET MGMTACL

Syntax

```
set mgmtacl id=value [ipaddress=ipaddress] [mask=string]
[application=telnet|web|ping|all]
```

Parameters

id	The identification number of the ACE to be modified. To view the ID numbers of the existing ACEs, refer to "SHOW MGMTACL" on page 670.
ipaddress	Specifies a new IP address for the ACE.
mask	Specifies a new mask for the ACE.
application	Specifies the permitted type of remote management. The options are: telnet — Permits Telnet management. web — Permits web browser management. ping — Permits the management workstation to ping the switch. all — Permits all of the above. You can specify more than one option by separating them with a comma (for example, "Web,Ping"). The new application replaces the current permitted application of the ACE.

Description

This command modifies an existing management access control entry in the Management ACL. You can use the command to change the IP address, subnet mask, or permitted applications of an ACE.

Examples

The following command changes the IP address of ACE ID 22 to 169.254.134.247:

```
set mgmtacl id=22 ipaddress=169.254.134.247
```

The following command changes the permitted applications of ACE ID 45 to web browser and pinging:

```
set mgmtacl id=45 application=web,ping
```

SHOW MGMTACL

Syntax

```
show mgmtacl [id=value]
```

Parameters

id Specifies the ID number of an ACE to view.

Description

This command displays the state of the Management ACL and ACL entries. Figure 60 is an example of the information displayed by this command.

```
 Management ACL Status ..................... Disable

ID    IP Address       Mask                Application
 ------------------------------------------------------------
 1    149.44.44.44     255.255.255.255     TELNET
 2    149.55.55.0      255.255.255.0       ALL
```

Figure 60. SHOW MGMTACL Command with ENTRIES Option

For an explanation of the parameters, refer to “CREATE MGMTACL” on page 663.

Examples

The following command displays the status of all the ACEs in the Management ACL:

```
show mgmtacl
```

The following command displays just the details of ACE ID 14:

```
show mgmtacl id=14
```

Index

Numerics

802.1Q multiple VLAN mode 526
802.1x Port-based Network Access Control 592
    authenticator port
        configuring 582
        displaying 594
    disabling 578
    displaying 594, 596
    enabling 580
    supplicant port
        configuring 590
        displaying 594

A

access control
    authenticator port, displaying 594
    supplicant port, displaying 594
access control entries (ACE)
    deleting 668
access control entry (ACE)
    adding 662
    creating 663
    deleting 665
    displaying 670
    modifying 669
access control list (ACL)
    creating 290
    deleting 292, 293
    displaying 296
    modifying 294
ACCESS SWITCH command 82
ACL. *See* access control list (ACL) and Management ACL
ACTIVATE MSTP command 490
ACTIVATE RSTP command 476
ACTIVATE STP command 462
ACTIVATE SWITCH PORT command 122
ADD LACP PORT command 178
ADD LOG OUTPUT command 250
ADD MGMTACL command 662
ADD MSTP command 491
ADD PKI CERTIFICATE command 622
ADD QOS FLOWGROUP command 310
ADD QOS POLICY command 311
ADD QOS TRAFFICCLASS command 312
ADD RADIUSSERVER command 650
ADD SNMP COMMUNITY command 102
ADD SNMPV3 USER command 397, 446
ADD SNTPSERVER PEER|IPADDRESS command 90
ADD SWITCH FDB|FILTER command 156
ADD SWITCH TRUNK command 168
ADD TACACSSERVER command 652
ADD VLAN command 516
ADD VLAN GROUP command 548
ADD VLAN MACADDRESS command 558
ADD VLAN PORT MACADDRESS command 559
ADD VLAN TYPE=MACADDRESS command 560
Address Resolution Protocol (ARP) table
    configuring timeout value 201
aging timer 161
AT-S63 software image
    downloading 226, 228, 232
    uploading 236, 238, 243, 246
AT-S63 software, resetting to factory defaults 54
authentication
    disabling 655
    displaying 660
    enabling 656
    protocol, selecting 658
    resetting to defaults 657
authentication failure traps
    disabling 111
    displaying 118
    enabling 114
authenticator port
    configuring 582
    displaying 594, 596

B

back pressure 131
boot configuration file names, displaying 222
BOOTP
    disabling 43, 44
    enabling 46, 48
    status, displaying 72
BPDU 481, 499
bridge forwarding delay 466, 480, 498
bridge hello time 466, 480, 498
bridge max age 466, 480, 498
bridge priority 466
broadcast filter 131

C

cache timeout 638
certificate database 633
certificates
    name, changing 631
    trust level, changing 631
CIST priority 501

Class of Service. *See* CoS
classifiers
creating 278
deleting 282, 283
displaying 287
modifying 284
removing from flow group 328
CLEAR SCREEN command 32
CLEAR SNMPV3 ACCESS command 399
CLEAR SNMPV3 COMMUNITY command 401
CLEAR SNMPV3 NOTIFY command 402
CLEAR SNMPV3 TARGET ADDR command 403
CLEAR SNMPV3 VIEW command 404
command line prompt 38
commands, formatting 28
compact flash card
configuration file on 219
copying files 210
directory, selecting 218
displaying files 223
files on 221
renaming files 216
space available 221
configuration file
creating 212
downloading 228, 232
name 222
setting 219
uploading 238, 243, 246
console mode, setting 39
console timeout 63
console timer, setting 63
contact name, configuring 53, 64
COPY command 210
CoS
Class of Service priority
setting 303
specifying 300
mapping to egress queues 300, 303
QoS scheduling 304
CREATE ACL command 290
CREATE CLASSIFIER command 278
CREATE CONFIG command 212
CREATE ENCO KEY command 614
CREATE LACP AGGREGATOR command 179
CREATE LOG OUTPUT command 252
CREATE MGMTACL command 663
CREATE MSTP command 492
CREATE PKI CERTIFICATE command 624
CREATE PKI ENROLLMENTREQUEST command 627
CREATE QOS FLOWGROUP command 313
CREATE QOS POLICY command 316
CREATE QOS TRAFICCLASS command 323
CREATE SNMP COMMUNITY command 104
CREATE SNMPV3 ACCESS command 405
CREATE SNMPV3 COMMUNITY command 408
CREATE SNMPV3 GROUP command 410
CREATE SNMPV3 NOTIFY command 412
CREATE SNMPV3 TARGETADDR command 414
CREATE SNMPV3 TARGETPARAMS command 416
CREATE SNMPV3 VIEW command 418
CREATE SWITCH TRUNK command 170
CREATE VLAN command 518
CREATE VLAN PORTPROTECTED command 550

D

daylight savings time, setting 96
default gateway, displaying 74
DELETE FILE command 213
DELETE IP ARP command 198
DELETE LACP PORT command 181
DELETE MSTP command 493
DELETE PKI CERTIFICATE command 629
DELETE QOS FLOWGROUP command 328
DELETE QOS POLICY command 329
DELETE QOS TRAFFICCLASS command 330
DELETE RADIUSSERVER command 653
DELETE SNMP COMMUNITY command 107
DELETE SNMPV3 USER command 420
DELETE SNTPSERVER PEER|IPADDRESS command 91
DELETE SWITCH FDB|FILTER command 158
DELETE SWITCH TRUNK command 172
DELETE TACACSSERVER command 654
DELETE TCP command 199
DELETE VLAN command 521, 551
DELETE VLAN MACADDRESS command 562
DELETE VLAN PORT MACADDRESS command 563
Denial of Service. *See* DoS
DESTROY ACL command 292
DESTROY CLASSIFIER command 282
DESTROY ENCO KEY command 618
DESTROY LACP AGGREGATOR command 182
DESTROY LOG OUTPUT command 256
DESTROY MGMTACL 665
DESTROY MSTP MSTIID command 494
DESTROY QOS FLOWGROUP command 331
DESTROY QOS POLICY command 332
DESTROY QOS TRAFFICCLASS command 333
DESTROY SNMP COMMUNITY command 109
DESTROY SNMPV3 ACCESS command 421
DESTROY SNMPV3 COMMUNITY command 423
DESTROY SNMPV3 GROUP command 424
DESTROY SNMPV3 NOTIFY command 425
DESTROY SNMPV3 TARGETADDR command 426
DESTROY SNMPV3 TARGETPARAMS command 427
DESTROY SNMPV3 VIEW command 428
DESTROY SWITCH TRUNK command 173
DESTROY VLAN command 523, 553, 564
DHCP
disabling 43, 44
enabling 47, 48
status, displaying 72
DISABLE AUTHENTICATION command 655
DISABLE DHCPBOOTP command 43
DISABLE GARP command 534
DISABLE HTTP SERVER command 604
DISABLE IGMPSNOOPING command 370
DISABLE INTERFACE LINKTRAP command 123

DISABLE IP REMOTEASSIGN command 44
DISABLE LACP command 183
DISABLE LOG command 257
DISABLE LOG OUTPUT command 258
DISABLE MGMTACL command 666
DISABLE MLDSNOOPING command 380
DISABLE MSTP command 495
DISABLE PORTACCESS|PORTAUTH command 578
DISABLE RADIUSACCOUNTING command 579
DISABLE RRPSNOOPING command 390
DISABLE RSTP command 477
DISABLE SNMP AUTHENTICATETRAP command 111
DISABLE SNMP command 110
DISABLE SNMP COMMUNITY command 112
DISABLE SNTP command 92
DISABLE SSH SERVER command 642
DISABLE STP command 463
DISABLE SWITCH PORT command 124
DISABLE SWITCH PORT FLOW command 125
DISABLE TELNET command 45
distinguished name
  displaying 79
  setting 634
document conventions 17
DoS
  displaying 364
  IP Option defense 355
  LAND defense 354, 357
  Ping of Death defense 358
  SMURF defense 354, 360
  SYN ACK Flood defense 361
  Teardrop defense 362

E

edge port 483, 505
ENABLE AUTHENTICATION command 656
ENABLE BOOTP command 46
ENABLE DHCP command 47
ENABLE GARP command 535
ENABLE HTTP SERVER command 605
ENABLE IGMPSNOOPING command 371
ENABLE INTERFACE LINKTRAP command 126
ENABLE IP REMOTEASSIGN command 48
ENABLE LACP command 184
ENABLE LOG command 259
ENABLE LOG OUTPUT command 260
ENABLE MGMTACL command 667
ENABLE MLDSNOOPING command 381
ENABLE MSTP command 496
ENABLE PORTACCESS|PORTAUTH command 580
ENABLE RADIUSACCOUNTING command 581
ENABLE RRPSNOOPING command 391
ENABLE RSTP command 478
ENABLE SNMP AUTHENTICATETRAP command 114
ENABLE SNMP command 113
ENABLE SNMP COMMUNITY command 115
ENABLE SNTP command 93
ENABLE SSH SERVER command 643
ENABLE STP command 464
ENABLE SWITCH PORT command 127
ENABLE SWITCH PORT FLOW command 128
ENABLE TELNET command 49
ENCO module, displaying 620
encryption key
  configuring 619
  creating 614
  destroying 618
enhanced stacking
  management session 82
  switch list, displaying 86
  switch mode, setting 84
event log
  configuring 264
  disabling 257
  displaying 268, 275
  enabling 259
  resetting to defaults 261
  saving 262
EXIT command 33
external port cost 505

F

factory defaults 54
files
  copying 210
  deleting 213
  displaying file list 223
  downloading 228, 232
  renaming 216
  uploading 238, 243, 246
flash memory
  configuration file in 219
  copying files 210
  displaying files 223
  files in 224
  formatting 215
  renaming files 216
  space available in 224
flow control
  disabling 125
  enabling 128, 131
flow group
  adding classifiers to 310
  creating 313
  modifying 328
  removing from traffic class 330
force version 480, 498
forwarding delay 466, 480, 498

G

GARP
  converting dynamic VLANs 528
  counters, displaying 541
  database, displaying 543
  disabling 534
  displaying 540
  enabling 535
  GID state machines 545

GIP 544
port GVRP status 537
resetting to defaults 536
timer, setting 538
gateway address
displaying 75
resetting to default 51
setting default 60
GID state machines 545
GIP-connected ring 544

H

head of line blocking 133
hello time 466, 480, 498
help, context-sensitive 27
HOL blocking 131
HTTP server
configuring 607
disabling 604
displaying 612
enabling 605
resetting to defaults 606

I

IGMP snooping
configuring 372
disabling 370
displaying 375, 376
enabling 371
ingress filtering 524
internal port cost 505
IP address
displaying 74
resetting to default 51
setting 58
IPOPTION denial of service defense 355

K

keyword abbreviations 27

L

LACP
disabling 183, 188
displaying status 189
enabling 184, 188
LACP aggregator
adding ports 178
changing adminkey 185
changing load distribution method 185
creating 179
deleting ports 181
destroying 182
displaying status 189
setting system priority 187
LAND denial of service defense 357
LOAD METHOD=LOCAL command 226
LOAD METHOD=TFTP command 228
LOAD METHOD=XMODEM command 232
location, configuring 53, 64
log output
adding 250
creating 252
destroying 256
disabling 258
displaying 273
enabling 260
modifying 265
LOGOFF command 35
LOGOUT command 35

M

MAC address aging timer 161
MAC address table
addresses
adding 156
deleting 158, 160
displaying 163
aging time 161
multicast groups 372, 382
MAC address-based VLAN
adding egress ports 559
adding MAC addresses 558
creating 560
deleting 564
deleting egress ports 563
deleting MAC addresses 562
displaying 565
MAC addresses
adding 156
deleting 158, 160
Management ACL
access control entry
adding 662
creating 663
deleting 665, 668
modifying 669
disabling 666
displaying 670
enabling 667
management VLAN, setting 525
manager password, setting 61, 66
MAP QOS COSP command 300
master switch 84
max age 466, 480, 498
max hops 498
Mcheck 483, 505
MDI mode 131
MENU command 36
migration check 483, 505
MLD snooping
configuring 382
disabling 380
displaying 384, 386
enabling 381
MSTI ID
adding 491
creating 492
deleting 493, 494

MSTI priority 502
MSTP
activating 490
disabling 495
displaying 509
enabling 496
returning to defaults 497
setting 498
VLAN association 504
multicast router port 372, 382
multiple VLAN mode 526

N

NULL character 65, 78

O

operator password, setting 62, 66

P

packet filtering 135
PING command 50
PING OF DEATH denial of service defense 358
PKI certificate database 633
PKI certificate enrollment request
creating 627
PKI certificates
adding 622
creating 624
deleting 629
displaying 636
downloading 228, 232
number of certificates 635
uploading 243, 246
PKI module information 635
PKI, resetting to defaults 630
point-to-point port 483, 505
policy
adding traffic classes to 311
creating 316
port
autonegotiation, setting 122
back pressure
disabling 132
enabling 132
back pressure, limit 133
broadcast filter 133
configuring 131
cost 469, 483
description, setting 131
disabling 124
displaying parameters 143
enabling 127
flow control
disabling 125
enabling 128
GVRP status, setting 537
head of line blocking 133
interface information 141
link traps
disabling 123
enabling 126
negotiation 131
packet filitering 135
priority 469, 483, 505
rate limit 138
resetting 130, 133
security 570, 571, 574, 575
speed, setting 131
statistics counter
displaying 154
resetting 150
status, specifying 131
port intrusion action 570
port mirror
destination port, setting 194
displaying 196
setting 195
port trunk
adding 168
creating 170
deleting 172
destroying 173
displaying 175
load distribution 174
setting 174
speed, setting 174
port-based access control
authenticator port, configuring 582
disabling 578
displaying 594, 596
enabling 580
RADIUS accounting 592
supplicant port, configuring 590
port-based VLAN
adding ports 516
creating 518
deleting ports 521
destroying 523
displaying 529
protected ports VLANs
adding ports 548
changing port type 554
creating 550
deleting 553
deleting ports 551
displaying 555
PURGE ACL command 293
PURGE AUTHENTICATION command 657
PURGE CLASSIFIER command 283
PURGE GARP command 536
PURGE HTTP SERVER command 606
PURGE IP command 51
PURGE LOG command 261
PURGE MGMTACL 668
PURGE MSTP command 497
PURGE PKI command 630
PURGE QOS COMMAND 302, 334
PURGE RSTP command 479

PURGE SNTP command 94
PURGE STP command 465

Q

QoS
    resetting to defaults 302, 334
QoS configuration, displaying 307
QoS flow group
    adding 310
    creating 313
    deleting 331
    displaying 347
    modifying 328, 335
QoS policy
    adding 311
    creating 316
    deleting 332
    displaying 349
    modifying 329, 338, 341
QoS traffic class
    adding 312
    creating 323
    deleting 333
    displaying 351
    modifying 330, 342
Quality of Service. *See* QoS
QUIT command 35

R

RADIUS accounting
    configuring 592
    disabling 579
    displaying 599
    enabling 581
RADIUS server
    adding 650
    deleting 653
rate limiting 138
RENAME command 216
RESET IP ARP command 200, 201
RESET SWITCH command 52
RESET SWITCH FDB command 160
RESET SWITCH PORT command 130
RESET SWITCH PORT COUNTER command 150
RESET SYSTEM command 53
RESTART REBOOT command 54
RESTART SWITCH command 55
round robin QoS scheduling 304
RRP snooping
    disabling 390
    displaying 392
    enabling 391
RSTP
    activating 476
    disabling 477
    displaying 486
    enabling 478
    port, setting 483
    resetting to defaults 479
    setting 480

S

SAVE CONFIGURATION command 37
SAVE LOG command 262
Secure Shell (SSH), configuration overview 644
serial terminal port
    settings, displaying 67
    speed, setting 57
SET ACL command 294
SET ASYN command 57
SET AUTHENTICATION command 658
SET CLASSIFIER command 284
SET CONFIG command 219
SET DATE TIME command 95, 97
SET DOS command 354
SET DOS IPOPTION command 355
SET DOS LAND command 357
SET DOS PINGOFDEATH command 358
SET DOS SMURF command 360
SET DOS SYNFLOOD command 361
SET DOS TEARDROP command 362
SET ENCO KEY command 619
SET GARP PORT command 537
SET GARP TIMER command 538
SET HTTP SERVER SECURITY command 607
SET IP IGMP command 372
SET IP INTERFACE command 58
SET IP ROUTE command 60
SET IPV6 MLD command 382
SET LACP AGGREGATOR command 185
SET LACP STATE command 188
SET LACP SYSPRIORITY command 187
SET LOG FULLACTION command 264
SET LOG OUTPUT command 265
SET MANAGER OPERATOR command 66
SET MGMTACL command 669
SET MSTP CIST command 501
SET MSTP command 498
SET MSTP MSTI command 502
SET MSTP MSTIVLANASSOC command 504
SET MSTP PORT command 505
SET PASSWORD MANAGER command 61
SET PASSWORD OPERATOR command 62, 66
SET PKI CERTIFICATE command 631
SET PKI CERTSTORELIMIT command 633
SET PORTACCESS|PORT AUTH PORT AUTHENTICATOR command 582
SET PORTACCESS|PORT AUTH PORT SUPPLICANT command 590
SET PROMPT command 38
SET QOS COSP command 303
SET QOS FLOWGROUP command 335
SET QOS POLICY command 338
SET QOS PORT command 341
SET QOS SCHEDULING command 304
SET QOS TRAFFICCLASS command 342
SET RADIUSACCOUNTING command 592
SET RSTP command 480

SET RSTP PORT command 483
SET SNMP COMMUNITY command 116
SET SNMPV3 ACCESS command 434
SET SNMPV3 COMMUNITY command 436
SET SNMPV3 GROUP command 438
SET SNMPV3 NOTIFY command 440
SET SNMPV3 TARGETADDR command 442
SET SNMPV3 TARGETPARAMS command 444
SET SNMPV3 VIEW command 448
SET SNTP command 96
SET SSH SERVER command 646
SET SSL command 638
SET STP command 466
SET STP PORT command 469
SET SWITCH AGINGTIMER|AGEINGTIMER command 161
SET SWITCH CONSOLEMODE command 39
SET SWITCH CONSOLETIMER command 63
SET SWITCH INFILTERING command 524
SET SWITCH MANAGEMENTVLAN command 525
SET SWITCH MIRROR command 194
SET SWITCH PORT command 131
SET SWITCH PORT FILTERING command 135
SET SWITCH PORT INTRUSION command 570
SET SWITCH PORT MIRROR command 195
SET SWITCH PORT PRIORITY OVERRIDEPRIORITY command 305
SET SWITCH PORT RATELIMITING command 138
SET SWITCH PORT SECURITYMODE command 571
SET SWITCH STACKMODE command 84
SET SWITCH TRUNK command 174
SET SWITCH VLANMODE command 526
SET SYSTEM command 64
SET SYSTEM DISTINGUISHEDNAME command 634
SET TELNET INSERTNULL command 65
SET VLAN command 528, 554
SHOW ACL command 296
SHOW ASYN command 67
SHOW AUTHENTICATION command 660
SHOW CLASSIFIER command 287
SHOW CONFIG command 222
SHOW CONFIG DYNAMIC command 68
SHOW CONFIG INFO command 71
SHOW DHCPBOOTP command 72
SHOW DOS command 364
SHOW ENCO command 620
SHOW FILE command 223
SHOW GARP command 540
SHOW GARP COUNTER command 541
SHOW GARP DATABASE command 543
SHOW GARP GIP command 544
SHOW GARP MACHINE command 545
SHOW HTTP SERVER command 612
SHOW IGMPSNOOPING command 375
SHOW INTERFACE command 141
SHOW IP ARP command 202
SHOW IP IGMP command 376
SHOW IP INTERFACE command 74
SHOW IP MLD command 386
SHOW IP ROUTE command 75, 203
SHOW LACP command 189
SHOW LOG command 268
SHOW LOG OUTPUT command 273
SHOW LOG STATUS command 275
SHOW MGMTACL command 670
SHOW MLDSNOOPING command 384
SHOW MSTP command 509
SHOW PKI CERTIFICATE command 636
SHOW PKI command 635
SHOW PORTACCESS|PORTAUTH command 594
SHOW PORTACCESS|PORTAUTH PORT command 596
SHOW QOS CONFIG command 307
SHOW QOS FLOWGROUP command 347
SHOW QOS POLICY command 349
SHOW QOS TRAFFICCLASS command 351
SHOW RADIUSACCOUNTING command 599
SHOW REMOTELIST command 86
SHOW RRPSNOOPING command 392
SHOW RSTP command 486
SHOW SNMP command 118
SHOW SNMPV3 ACCESS command 450
SHOW SNMPV3 COMMUNITY command 451
SHOW SNMPV3 GROUP command 452
SHOW SNMPV3 NOTIFY command 453
SHOW SNMPV3 TARGETADDR command 454
SHOW SNMPV3 TARGETPARAMS command 455
SHOW SNMPV3 USER command 456
SHOW SNMPV3 VIEW command 457
SHOW SNTP command 98
SHOW SSH command 648
SHOW SSL command 639
SHOW STP command 473
SHOW SWITCH AGINGTIMER|AGEINGTIMER command 162
SHOW SWITCH command 76
SHOW SWITCH COUNTER command 151
SHOW SWITCH FDB command 163
SHOW SWITCH MIRROR command 196
SHOW SWITCH PORT command 143
SHOW SWITCH PORT COUNTER command 154
SHOW SWITCH PORT INTRUSION command 574
SHOW SWITCH PORT SECURITYMODE command 575
SHOW SWITCH TRUNK command 175
SHOW SYSTEM command 79
SHOW TCP command 204
SHOW TIME command 100
SHOW USER command 40
SHOW VLAN command 529, 555, 565
slave switch 84
SMURF denial of service defense 360
SNMP
  disabling 110
  information, displaying 118
SNMP community
  adding 102
  creating 104
  deleting 107
  destroying 109

disabling 112
enabling 113, 115
modifying 116
SNMP management access 102
SNMPv3 Access Table entry
clearing 399
creating 405
deleting 421
modifying 434
SNMPv3 Community Table entry
clearing 401
creating 408
deleting 423
modifying 436
SNMPv3 Notify Table entry
clearing 402
creating 412
deleting 425
modifying 440
SNMPv3 SecurityToGroup Table entry
creating 410
deleting 424
modifying 438
SNMPv3 Target Address Table entry
clearing 403
creating 414
deleting 426
modifying 442
SNMPv3 Target Parameters Table entry
creating 416
deleting 427
displaying 455
modifying 444
SNMPv3 User Table entry
adding 397
deleting 420
displaying 456
SNMPv3 View Table entry
clearing 404
creating 418
deleting 428
displaying 457
SNTP
disabling 92
enabling 93
information, displaying 98
IP address
deleting 91
specifying 90
resetting to defaults 94
SSH configuration, displaying 648
SSH server
configuring 646
disabling 642
enabling 643
SSL
configuring 638
displaying 639
static multicast address 156
static unicast address 156
STP
activating 462
disabling 463
displaying 473
enabling 464
port, setting 469
resetting to defaults 465
setting 466
strict QoS scheduling 304
subnet mask
displaying 74
resetting to default 51
setting 58
supplicant port
configuring 590
displaying 594, 596
switch
accessing via enhanced stacking 82
configuration, displaying 68, 71, 222
distinguished name 79
information, displaying 79
parameters, displaying 76
restarting 55
statistics counters, displaying 151
SYNFLOOD denial of service defense 361
system date
displaying 100
setting 95, 97
system files
downloading 228, 232
uploading 238, 243, 246
system name, configuring 53, 64
system time
displaying 100
setting 95, 97

T

TACACS+ server
adding 652
deleting 654
tagged port
adding 548
deleting 551
tagged VLAN
adding ports 516
creating 518
deleting ports 521
destroying 523
displaying 529
TEARDROP denial of service defense 362
Telnet server
disabling 45
enabling 49
temperature, switch, displaying 79
traffic class
adding flow groups to 312
creating 323
removing from policy 329

trap receiver 102

U

untagged port
    adding 548
    deleting 551
UPLOAD METHOD=LOCAL command 236
UPLOAD METHOD=REMOTESWITCH command 238
UPLOAD METHOD=TFTP command 243
UPLOAD METHOD=XMODEM command 246
uploading files 238, 243, 246
UTC offset, setting 96

V

VLAN. *See* 802.1Q multiple VLAN mode, MAC address-based VLAN, multiple VLAN mode, port-based VLAN, protected ports VLAN, and tagged VLAN